Docket No.
105026/0002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: **Andrew Casper** Group Art Unit: **3628**

Application No.: **09/521,636** Examiner: **Poinvil, F.**

Filed: **March 8, 2000**

For: **SECURE TRANSACTION PROCESSING SYSTEM AND METHOD**

Date: **March 11, 2005**

CERTIFICATE OF MAILING
BY "FIRST CLASS MAIL" (37 C.F.R. § 1.8)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

I hereby certify that the following correspondence:

Petition for Extension of Time - 3 months (in duplicate); Request for Oral Hearing (in duplicate); Brief on Appeal & Declaration of Andrew Casper (in triplicate).

is being deposited on **MARCH 11, 2005** with the United States Postal Service as first class mail in an envelope bearing sufficient postage thereon and addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450.

RICHARD ESKEW
(Typed Or Printed Name Of Person Mailing Correspondence)

(Signature Of Person Mailing Correspondence)

UNITED STATES PATENT & TRADEMARK OFFICE

Application No.	:	09/521,636
Title	:	SECURE TRANSACTION PROCESSING SYSTEM AND METHOD
Applicant	:	Andrew Casper
Filed	:	March 8, 2000
TC/AU	:	3628
Examiner	:	Frantzy Poinvil
Docket No.	:	105026/0002

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

BRIEF ON APPEAL

Sir:

Applicant submits this Brief on Appeal (in triplicate) in response to the Final Rejection of September 13, 2004. The filing of this Brief on Appeal is timely as the due date with payment of appropriate extension fees under 37 C.F.R. 1.136(a) is March 13, 2005. A three month extension of time of the due date of the Final Rejection has been submitted herewith. The Commissioner is hereby authorized to charge the Small Entity Appeal Fee of $250.00, and any further fees or deficiencies in fees, to Deposit Account No. 19-4709. A Request for Oral Hearing is also submitted herewith.

Certificate of Mailing (37 C.F.R. 1.8)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450, on **March 11, 2005.**

Typed or printed name of person signing this certificate:

Richard Eskew

Signature

This Appeal is being taken in response to the Final Rejection, dated September 13, 2004, in which the Examiner finally rejected claims 1-6, 8-10, and 12-25, all of the claims currently pending in the subject Application. A Notice of Appeal was filed on December 13, 2004.

I. REAL PARTY IN INTEREST

The real party in interest in this case is Andrew Casper. No assignment of the present application has been executed.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellants, or their legal representatives which would directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal.

III. REQUEST FOR ORAL HEARING

An oral hearing is hereby requested.

IV. STATUS OF THE CLAIMS

By the outstanding Final Rejection, claims 1-6, 8-10, and 12-25, all of the claims currently pending in the subject Application, stand finally rejected.

Claim 7 was cancelled without prejudice.

V. STATUS OF THE AMENDMENTS

In the Final Rejection, dated September 13, 2004, the Examiner finally rejected claims 1-6, 8-10, and 12-25, all of the claims currently pending in the subject Application. No Amendment after Final has been filed. The Final Rejection was issued in response to an Amendment filed by Applicant on May 26, 2004.

VI. SUMMARY OF THE INVENTION

The present invention as set forth, for example, in independent claim 1 and 14 presents a novel system and method for facilitating the processing of secure electronic purchase transactions to thereby reduce the potential for credit card fraud and/or identity theft.

Specifically, a preferred embodiment of the present invention comprises a processing system that stores purchaser account information, such as a credit card number. The purchaser account information is stored in a purchaser account database. The purchaser account database stores purchaser account information including at least a purchaser identifier that is associated with and inextricably linked to delivery data such that any change or attempted change in the delivery data will render the purchaser identifier inoperable. The purchaser identifier is also linked to the payment data (e.g., a credit card number). The purchaser identifier is different from the payment data.

In processing a purchase order transaction that includes a purchaser identifier, the purchaser identifier is utilized to retrieve the associated delivery and payment data. The processor uses the payment data to pay for the purchased goods or services without exposing the payment data to the merchant. Specification at p. 5, ll. 7-15. So that the merchant can fulfill the purchase order (e.g., by shipping the purchased goods to the purchaser), the processor of the processing system transmits the delivery data corresponding to the purchaser identifier in the purchase order to the merchant.

The delivery data may comprise a physical delivery address, such as a postal mailing address or a post office box number, or an electronic address such as an e-mail address. The specification specifically discloses the effect of the system and method of the present invention, as follows:

> A unique purchaser identifier is assigned to each purchaser and linked to that purchaser's purchasing information which is stored in a purchaser account. The identifier – or personal identification number (PIN)—bears no relation to the purchaser's financial information. Only the identifier and the corresponding delivery information is communicated when purchases are made.

Specification at p. 5, ll. 16-19. Further, it is explained that:

> Furthermore, the purchaser identifier and the corresponding purchaser account cannot be changed at any time or by any party, including the purchaser, without that particular purchaser identifier

> and account being disabled. Once disabled the purchaser identified is void and a new identifier must be issued. The present invention, therefore, prevents unauthorized use of a purchaser's purchasing information by ensuring that any purchases are delivered only to the purchaser's physical or electronic address. Any fraudulent use of the purchaser identifier will be instantly revealed because the goods or electronic information must be delivered directly to the purchaser's delivery address. Because the purchaser will know whether a valid purchase has been made, the purchaser can suspend or disable the account without canceling credit or debit cards.

Specification at p. 6, ll. 4-13.

Thus, even if the purchaser identifier is stolen and used to attempt a fraudulent purchase, the products will be delivered only to the pre-defined delivery address associated with that identifier. In this way, fraudulent purchases will be recognized immediately by the user who can notify his/her credit card company, for example, to stop payment. If any attempt to change the delivery address is made, the account will be disabled. In this way, unlike the references cited by the Examiner, the purchaser has complete control over where purchases are delivered and someone stealing the purchaser's account identifier (e.g., a user ID, password, or PIN number) would be unable to change the delivery address. Moreover, because purchases are made without exposing or transmitting financially sensitive credit or debit card numbers to the Merchant, even if a thief or hacker were to intercept the purchasers identities, little to no harm to the purchasers' financial assets would be realized. Consequently, the fraudulently purchased article or piece of data or information, such as by way of example, an online software purchase or so called e-book, will be received by the purchaser at his or her specified delivery address and will thereby have notification of fraudulent use of his or her account.

Claims 8 and 11 further specify a "securitizer" which acts to minimize the chance of unauthorized access to the private network on which the processing system resides. The claimed securitizer in claims 8 and 11 is more than a so-called firewall that is commonly used to protect networks from outside interference or hacking. Here, the securitizer monitors the secure network

including the purchaser account database and the processor to detect any alterations or changes to the stored delivery data. Unlike a firewall, the securitizer will trigger the disabler to disable a particular purchaser identifier or purchaser accounts even if access to the system is the result of a valid purchaser identifier and not as a hack or break-in to the system. In this way, the securitizer is distinct from the commonly used and commonly known firewall.

Claim 17 sets forth a novel method for using the present invention in which a an account is set-up by a purchaser. Purchaser account information, including at least payment and delivery data, is stored and a unique purchaser identifier is generated. The purchaser identifier is inextricably linked to the stored delivery data. If an attempt to change the delivery data is detected, the purchaser identifier is rendered inoperable. Furthermore, to process a purchase order, the delivery and payment data associated with a purchaser identifier is retrieved and (i) payment is effected without exposing the payment data to the merchant and (ii) only the delivery data is communicated to the merchant.

Claim 20 sets forth a novel method for facilitating secure transactions wherein a purchaser selects a product to be purchased and enters and transmits his/her purchaser identifier to the merchant store system. The merchant store system generates a purchase order and communicates the purchase order to the processing system. The processing system then processes the purchase order by retrieving the payment and delivery data associated with the purchaser identifier. To process the purchase order, payment is effected without exposing the payment data to the merchant and the delivery data is communicated to the merchant.

Claim 25 sets forth a novel processing system for processing a secure purchase order between a purchaser and a merchant wherein the processing system resides on a private network and the merchant and purchaser computers reside on a public network. A purchaser account database also resides on the private network. The processing system is programmed to receive from the purchaser computer purchaser account information including at least delivery data

including at least one delivery address for the purchaser and payment data for effecting payment of purchased goods or services. The processing system stores the purchaser account information on the purchaser account database and generates a purchaser identifier that is an alpha-numeric code having no monetary value and that is unrelated to any personally identifiable information of the purchaser. The purchaser identifier is linked to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable. To process a purchase order from the purchaser, the processing system is further programmed to receive a purchase order, including order information and the purchaser identifier. The processing system, upon receipt of the purchase order, verifies the purchaser identifier and retrieves the payment data and the delivery data corresponding to the purchaser identifier from the purchaser account database. Payment is then arranged to be made to the merchant for the purchased goods or services without exposing the payment data to the merchant. The delivery data and a payment authorization to fulfill the purchase order is then transmitted to the merchant. At no point in the purchasing process is the purchaser required to enter or transmit the payment data at any time to make the purchase.

VII. THE ISSUES

1. Whether claims 1-6, 8-10, 12-19 and 25 are unpatentable under 35 U.S.C. 103 as being obvious over Lewis (U.S. Pat. No. 6,233,565) in view of Edwards ("Education is weapon against credit fraud") in further view of Walker et al. (U.S. Pat. No. 5,794,207).

2. Whether claims 20-21 are unpatentable under 35 U.S.C. 103 as being obvious over Egendorf (U.S. Pat. No. 6,188,994) in view of Edwards ("Education is weapon against credit fraud") in further view of Walker et al. (U.S. Pat. No. 5,794,207).

3. Whether claims 22-24 are unpatentable under 35 U.S.C. 103 as being obvious over Egendorf (U.S. Pat. No. 6,188,994) in view of Lewis (U.S. Pat. No. 6,233,565), Edwards ("Education is weapon against credit fraud"), and Walker et al. (U.S. Pat. No. 5,794,207).

VIII. GROUPING OF THE CLAIMS

Applicant respectfully submits that the Examiner's groupings of the claims for the purposes of the prior art rejections are improper. Applicant suggests that the claims should be grouped as follows.

Claims 1-6, 8-10, 12-16 stand and fall with the patentability of claim 1.

Claims 17-19 stand and fall with the patentability of claim 17. Claim 17, as well as the remainder of the claims in this group are method claims and separately set forth a novel method of facilitating secure transactions between a purchaser and a merchant. Claim 17 specifically claims the steps of generating the purchaser identifier so that the purchaser identifier is inextricably linked to the stored delivery data and rendering the purchaser identifier inoperable in response to any change or attempted change in the stored delivery data. Therefore, this group of claims presents an independently patentable group in that the group of claims sets forth a novel method which does not require the specific structural elements set forth in the system claims of the first group.

Claims 20-21 stand and fall with the patentability of claim 20. Because the Examiner has appropriately grouped claims 20-21 no change in the grouping is required.

Claims 22-24 stand and fall with the patentability of claim 22. Because the Examiner has appropriately grouped claims 22-24 no change in the grouping is required.

Claim 25 should be set forth in its own group. The Examiner improperly grouped claim 25 with the first group stemming from independent claims 1 and 14. Claim 25 separately sets forth that the processing system resides on a private network and is in communication with purchaser and merchant computers via a public network. Claim 25 also separately defines that the processing system is programmed to "verify the purchaser identifier and retrieve the payment data and the delivery data corresponding to the purchaser identifier from the purchaser account database," which also resides on the private network. Therefore, this group of claims presents an

independently patentable group in that the group of claims sets forth a novel method which does not require the specific structural elements set forth in the system claims of the first group.

IX. ARGUMENT

A. REJECTION UNDER 35 U.S.C. § 103(A) - LEWIS ET AL., U.S. PATENT NO. 6,233,565 IN COMBINATION WITH EDWARDS AND WALKER, ET AL., U.S. PATENT NO. 5,794,207.

1. Even If The Combination Of Lewis, Edwards And Walker Is Proper, Which It Is Not, The Examiner Has Failed To Present A *Prima Facie* Case Of Obviousness.

Pursuant to M.P.E.P. 2142, the Examiner bears the initial burden of establishing a *prima facie* case for obviousness. "If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." M.P.E.P. 2142 (emphasis in original). Specifically, the MPEP sets forth the following criteria for the establishment of the prima facie case of obviousness:

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.

Id. (emphasis in original). Moreover, "[t]o support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985). *See* MPEP §

2144 - § 2144.09 for examples of reasoning supporting obviousness rejections. The Examiner has failed to meet this burden on all accounts.

First, the Examiner's sole basis for the combination of Lewis (a reference directed to a specialized mail postage purchasing system using encryption) with Walker (a reference directed at a reverse auction process for online purchases, e.g., priceline.com) and Edwards (an article imploring travel agents to physically match credit card numbers to the name and billing address on file for the cardholder) is that "fraud prevention is well known." Under the Examiner's rationale every reference discussing fraud (and there must be thousands) could be combined with any other reference even if the two references employ wholly different approaches to the solution. This is not the law.

The motivation or suggestion to combine the references must come from the references themselves, and not from the inventor's application. Moreover, "the level of skill in the art cannot be relied upon to provide the suggestion to combine references. *Al-Site Corp. v. USI International, Inc.*, 174 F.3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999)." MPEP 2143.01. "Where the teachings of two or more references conflict, the examiner must weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another." *Id.* In this case, the Examiner has pointed to a general desire to prevent fraud for the motivation to combine. Specifically, the Examiner states:

> Lewis et al. teaches disabling the purchaser identifier (column 3, lines 38-42) **in response to a fraud not to a specific fraud** such as the delivery data associated with a particular purchaser identifier. Final Rejection at 6 (emphasis added).

This statement evidences the Examiner's failure to consider the fact that Lewis teaches fraud prevention through complex encryption techniques for the transmission of sensitive data online, whereas Edwards concerns credit card address verification for in-person or over the phone transactions. The two references are not only non-analogous, but also provide conflicting

teachings; namely, encrypting sensitive data versus manually checking for a matching billing address.[1] The Examiner has ignored these differences asserting only, "[t]he motivation would have been to prevent fraudulent transactions from occurring as noted by Edwards." Final Rejection at 6.

Given the conflicting, non-analogous teachings of Lewis and Edwards, the Examiner's Statement of motivation is plainly deficient. Moreover, although discussed in detail below, the Examiner concedes that Lewis fails to disclose the claim limitation of inextricably linking the purchaser identifier to delivery data. The Examiner then contends that Edwards, which speaks of verifying a billing address, fills in the missing gap. Instead of making the Examiner's rejection, the disparate teachings of Lewis and Edwards highlight the novel system developed by Mr. Casper in which a delivery address is linked to a purchaser identifier (which is not financially sensitive) so that goods can only be delivered to that address. This is a wholly different approach as compared to the prior art.

Second, the Examiner has failed to show that the references in combination teach or suggest all the claim limitations at issue. The specific failings of the references are dealt with below.

---

[1] The phrase "billing address" is emphasized because it illustrates a general misunderstanding on the part of the Examiner. In Edwards and other credit card fraud prevention schemes, the billing address is used to verify that the person using the card is actually the owner of the card. This assumes that the credit card holder is providing both the card number and billing address to the merchant, in this instance, a travel agent. This is directly contrary to the claims of the present invention which expressly define a system that avoids exposing sensitive financial information to the merchant. Moreover, Edwards fails to provide a solution for when a thief steals the credit card statement or intercepts an Internet purchase that includes both the number and the billing address. In that event, the thief can present the proper number and billing address and have the fraudulently purchased goods shipped anywhere in the world. Edwards, and for that matter Lewis and Walker, simply do not solve this problem. In contrast, the present invention eliminates the need to transmit credit card and billing address information over the Internet, thereby eliminating a main cause of identity theft and fraud. Moreover, even if the purchasing identifier is intercepted, the fraudulent activity will likely be thwarted because the goods can only be shipping to the pre-stored delivery address. If the thief attempts to change this address, the purchaser identifier can no longer be used. This novel approach is not taught or suggested by the references cited.

2. **Lewis Fails To Teach Or Suggest The Features Of Claims 1, 14, and 17, As Amended.**

Despite the Applicant's amendments prior to the Final Rejection, the Examiner maintained the prior rejection based on Lewis; namely, that Lewis teaches "disabling the purchaser identifier (col. 3, lines 38-42) in response to a fraud," but does not teach disabling the purchaser identifier in response to "a specific fraud such as the delivery data associated with a particular purchaser identifier". Notwithstanding the Examiner's concession that Lewis fails to teach linking delivery data with a purchaser identifier, the Examiner asserts the following:

> [I]t would have been obvious to one of ordinary skill in the art that such a particular fraud detection measure would have constantly been monitored in the system of Lewis et al. because it has been known that hackers or thieves usually perform this type of fraud by having items or goods which they did not purchase or pay for being delivered at their desired address.

Final Rejection at 3. Applicant submits that Lewis' general fraud detection measures using primarily complex encryption techniques neither teaches nor suggests the system and method of the present claims.

a. **Lewis Is Not Analogous To The Present Invention And Fails To Teach Or Suggest Several Elements Of The Subject Claims.**

Lewis does not teach or suggest several features of the processing system of independent claims 1, 14, 17, 20, 22, and 25, and even if combined with Edwards and Walker cannot render said claims obvious.

i. ***Lewis is directed to a non-analogous type of purchasing system and employs a wholly different approach to fraud prevention, as compared to the subject claims, as amended.***

Lewis describes an electronic postage system that works in conjunction with Postal Security Device ("PSD") software residing on a Remote Service Provider ("RSP") server. The system of Lewis is very specialized and designed to process the purchase of postage from a

specified postal service, such as the U.S. Postal Service ("USPS"). Because postal services employ specialized regulations and specifications, the system of Lewis was designed to comply with this specialized set of regulations and specifications. For example, Lewis states that the USPS uses the Information Based Indicia Program ("IBIP"). Lewis, col. 1, lines 50-62. Although it is acknowledged that the system of Lewis could be modified to comply with the specific regulations of other postal service entities in Europe or Canada, for example, the Lewis system nevertheless is designed to permit postage purchases from a specific postal entity, such as the USPS, using specialized rules, such as IBIP. The Lewis system, therefore, is not analogous to the systems and methods of the present claims.

In particular, in Lewis, the user must download specialized software that permits the user to communicate with the RSP 4, as follows:

> User 2n makes a purchase through a proprietary connection over the Internet 30 using the appropriate IP address as provided by the downloaded client software to connect with the RSP's Internet transaction server 180, utilizing a suitable form of payment, such as credit cards, or checks.

Lewis, col. 12, lines 14-20. As a result, the postage purchasing system of Lewis would not be suitable as a general merchant purchasing system due to the specialized nature of Lewis' communications and security system. As will become evident from the following discussion, the specialized client software and RSP transaction server 180 operates in a wholly different manner from the systems and methods of the present claims.

ii. ***Lewis teaches away from the systems and methods of the present claims in that Lewis requires transmission of payment information via the Internet.***

Lewis fails to disclose, teach or suggest the claimed feature of "us[ing] the payment data to pay for the purchased goods or services without exposing the payment data to the merchant." In Lewis, in order to purchase postage, a "suitable form of payment, such as credit cards, or

checks" is required to be transmitted to the RSP's transaction server 180. *See id.* Specifically, Lewis describes the purchase request, as follows:

> **The customer then initiates transmission of all of the purchase information (e.g., addresses, purchase amount, and credit/check information) via the Internet 30 to the web server 150, which passes the transaction request to the transaction server 180.** When the Submit radio button is pressed, all customer information is digitally signed and encrypted and packaged with the purchase amount.... Because the transmission has the appropriate IP address for the transaction server 180 it will be directed by web server 150 through the firewall 160 to transaction server 180, where the transaction will be executed.

Lewis, col. 16 lines 18-20 (emphasis added). It is clear, therefore, that in order to pay for postage in the Lewis system (except where a check is used) a user must transmit their credit/debit card number to the transaction server 180 over the Internet. This is confirmed again in Lewis at col. 14, lines 25-42, wherein it states that the RC2 symmetric encryption "will be used to protect the nature of the purchase/refund request, which may include credit card information." *See also* Lewis, col. 16, lines 5-22. Again at col. 17, lines 4-15, Lewis describes the transmission of credit card numbers over the Internet:

> Credit card requests are transmitted to the web server 150 by the client, forwarded to the transaction server 180, and then to a payment server 190, a credit authorization server 400, and to a remote credit bureau 9 such as First Data Merchant Services ("FDMS").

By virtue of its chosen method of operation, the Lewis system is subject to potential interception of sensitive and valuable credit/debit card numbers. Lewis attempts to solve this problem by using encryption of the data transmission that contains the financially sensitive data, which is entirely different from the approach presented by the present invention.[2]

---

[2] For the sake of clarification, Applicant is not arguing that encryption methods cannot be used within the scope of the present invention, but rather that the present invention achieves its fraud protection via a novel approach of using a purchaser identifier inextricably linked to pre-stored delivery addresses that cannot be changes without rendering the purchaser identifier inoperable.

The Examiner's assertion that Lewis discloses processing payments without exposing the payment data to the merchant thus, is simply wrong. Final Rejection at 4. The following is the disclosure identified by the Examiner as disclosing the processing of payments without exposing payment data to the merchants:

> Preferably, the system also includes a third party seller having a processor and a database, and a communication channel between the third party seller and the server, wherein the client further comprises a registration certificate representative of being a consumer registered with said third party seller. In such a system, a transaction module is provided and the third party seller database is updated by said server transaction database.
>
> In an alternate embodiment, the system optionally may include a third party credit facility and a communication link between the third party credit facility and the server, wherein the server has a credit module and, in response to a suitable client transaction request, a credit card payment request is made by the server to the third party credit facility, the third party credit facility authorizes the credit card payment and issues an authorization code to the server, and the server transaction database is appropriately updated.

This disclosure fails to clearly teach a system in which credit card information is not exposed to merchants. In the context of the Lewis disclosure, both the server operated by a postal entity (e.g., the USPS) and the third party seller (e.g., Fedex) are merchants. Contrary to the Examiner's suggestion the third party credit facility is the entity responsible for authorizing credit card payments on behalf of a third party seller. According to Lewis, when a user desired to make a purchase of postage or to purchase the services of a third party seller, the user would transmit credit card data to the server. Lewis, col. 17:4-15. The server would then transmit the credit card data to the third party credit card facility for authorization. The transmission of credit card data over the Internet to make purchases teaches away from the present invention.

Lewis, thus, fails to disclose, teach or suggest the claimed feature of "us[ing] the payment data to pay for the purchased goods or services without exposing the payment data to the merchant."

iii. ***Lewis fails to disclose, teach or suggest use of a "purchaser identifier" in lieu of credit/debit card numbers to make purchases with various merchants.***

The systems and methods of claims 1, 14, 17, 20, 22 and 25, provide a user/purchaser with a purchaser identifier, which includes no financially usable information (e.g., credit card numbers or the like) and cannot be used to make purchases with any system other than the transaction processing system of the claims, to make purchases with any online merchant system, such as, by way of example, Amazon.com or CircuitCity.com.

With respect to the lack of a teaching or suggestion of a purchaser identifier, in Lewis, the user is identified through interaction of the downloaded client software and the transaction server 180. Lewis, therefore, neither teaches nor suggests use of a purchaser identifier that is an alpha-numeric code that is not the purchaser's credit or debit card number or other financially sensitive information. In contrast, Lewis requires the transmission of financially sensitive information each time a purchase is to be made.

Moreover, Lewis describes an initial registration procedure in which the user enters certain preliminary information. *See* Lewis, col. 11, lines 13-63. This information may include an address for the user. *Id.* Lewis, however, makes no teaching or suggestion that this address will be inextricably linked to a specific purchaser identifier or that the shipping address cannot be changed without disabling the purchasing system, and specifically the purchaser identifier as set forth in claims 1, 14, 17, 20, 22, and 25. In Lewis the thing being purchased is a monetary postage value. The postage value is not delivered to the customer, but rather is stored at the RSP server 4 in a descending register account for the customer. Thus, the addresses discussed in Lewis refer to mail delivery addresses used by the system of Lewis to calculate the amount of postage necessary to send a customer's mail. In contrast, the claims of the present invention are directed to a system in which purchased goods or services will be physically or electronically delivered to a pre-stored customer's delivery address. Thus, the system of Lewis is non-analogous to the present invention and fails to disclose, teach, or suggest the features of claims 1,

14, 17, 20 and 25 as amended, of using a purchaser identifier that is inextricably linked to a delivery address.

Lewis fails to disclose, teach or suggest the purchaser identifier of claim 1, as amended, and further fails to disclose, teach or suggest linking the purchaser identifier to a delivery address that cannot be changed. Moreover, Lewis teaches transmitting credit card information or the like over the Internet to make postage purchase, whereas the claims of the present invention, as amended, set forth that no such financial information is transmitted across the Internet.

As such, the claims, as amended, present a novel online purchase processing system that (1) reduces the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received, and (2) reduces the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only pre-stored delivery addresses.

Applicant, therefore, respectfully submits that the claims 1-6 and 8-10, and 12-19 are allowable as amended over the Lewis reference.

3. **Edwards And Walker Do Not Teach Or Suggest Inextricably Linking Delivery Data To A Purchaser Identifier.**

The Examiner concedes that Lewis does not teach the claimed feature "wherein the purchaser identifier is generated by the processing system during storage of the delivery data in the purchaser account database and is inextricably linked to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable". Final Rejection at 6. Nevertheless, the Examiner cites to the Edwards and Walker references as teaching this feature. Applicant submits that neither Edwards nor Walker teach or suggest the feature of inextricably linking a delivery address to a purchaser identifier to be used to make purchases.

a. **Edwards Is Not Analogous To And Should Not Be Combined With Lewis.**

Edwards is an article that advises travel agents on how to avoid becoming credit card fraud victims by verifying a credit card holder's billing address using an address verification system. Edwards does not present an electronic purchasing system, but rather is directed to the purchase of airline tickets over the phone. Edwards describes a scenario where the consumer gives the travel agent a credit card number and a billing address. The travel agent uses an address verification system to attempt to match the address to the card number. If the billing address does not match the address stored by the credit card company, Edwards advises the travel agent to deny the transaction. Because Edwards is not directed to the field of electronic commerce over the Internet, there would be no motivation to combine Edwards with Lewis.

b. **Edwards Fails To Disclose, Teach Or Suggest The Feature Of Inextricably Linking A Delivery Address To A Purchaser Identifier.**

Even if Edwards is combined with Lewis, as suggest by the Examiner, the combination would not render the claims, as amended, obvious. Notwithstanding the numerous deficiencies of Lewis as described above, Edwards fails to teach or suggest inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable. First, Edwards makes no teaching of a purchaser identifier that is different from any financially sensitive information, such as a credit card number. In contrast, in Edwards the purchaser's credit card number and billing address must be given directly to the merchant (travel agent) so that the information can be verified, which is exactly opposite to the systems and methods of the present claims.

Second, Edwards only crosschecks a billing address with the stored address of the credit card consumer, and makes no mention of any delivery address for the tickets. If the billing address matched (such as in the case where a hacker intercepted an online purchase including both a consumer's credit card number and billing address), the hacker would be able to send the airline tickets to any shipping address chosen by the hacker. This is because in heretofore known

electronic commerce systems, the ability to change delivery addresses was viewed as being advantageous so that the purchaser could ship the goods to any desired address. As such, if the purchaser desired to send someone a gift, the purchaser could easily do so by changing the shipping address to that of the person receiving the gift. The claims of the present application, however, set forth an entirely opposite approach where the purchaser is not given the option to change the delivery addresses, so that the incentive for a thief to steal the purchaser identifier is greatly reduced. In such a system, for instance, even if a consumer's purchaser identifier is stolen, a potential thief would have no incentive to use the purchaser identifier because the thief could not change the pre-stored delivery addresses without rendering unusable the purchaser identifier. Thus, even if the thief purchased goods, the goods would be delivered to the account owner's pre-stored delivery address and the account owner would quickly recognize the fraud and have an opportunity to take action.

Therefore, because Edwards fails to teach or suggest a purchaser identifier and the linking of the purchaser identifier to a delivery address, Edwards fails to render the claims obvious even if combined with Lewis.

c. **Walker Fails To Teach Or Suggest Inextricably Linking The Delivery Data To The Purchaser Identifier Such That Any Change Or Attempted Change To The Delivery Data Will Render The Purchaser Identifier Inoperable.**

While Walker is directed to an electronic commerce system, Walker also fails to teach or suggest inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable.

In the passages of Walker identified by the Examiner, namely col. 8:66-9:30 and 13:1-19, Walker describes usage of a unique ID number to identify the buyer. Walker, however, does not teach or suggest inextricably linking the ID number to a delivery address for the delivery of goods or services. Moreover, Walker fails to teach or suggest that a change or attempted change in the delivery address would result in the ID number being rendered inoperable. In contrast,

Walker only describes storing the buyer's address for registration purposes, which is presumably the buyer's billing address, but does not otherwise discuss storing or linking a delivery address to the ID number. Indeed, in Walker at col. 12, lines 31-49, where the exchange of goods between buyer and seller are described, there is no mention that the goods are required to be delivered to a pre-stored delivery address because the delivery address is linked to the ID number. Thus, Walker fails to teach or suggest the claimed feature of inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable. Thus, the ID number of Walker is very different from the purchaser identifier of the subject claims

As such, neither of the combinations suggested by the Examiner in rejecting the claims, even if such combination was, which it is not, render the claims obvious. In light of the above arguments and amendments to the claims, Applicant respectfully requests that the Examiner withdraw the rejection.

B. **REJECTIONS UNDER 35 U.S.C. § 103(A) OVER EGENDORF, U.S. PATENT NO. 6,188,994 IN VIEW OF LEWIS ET AL., U.S. PATENT NO. 6,233,565, EDWARDS AND WALKER, ET AL., U.S. PATENT NO. 5,794,207.**

The Examiner also rejected claims 20-21 over U.S. Patent No. 6,188,994 to Egendorf in view of Edwards and Walker, and claims 22-24 as being obvious over Egendorf in view of Lewis, Edwards, and Walker.

With respect to these rejections, the Examiner concedes that Egendorf does not teach or suggest the features "wherein the purchaser identifier is inextricably linked to the delivery data..." (claim 20) and "once the secure consumer account is established by the consumer and the unique customer identifier is assigned to the customer account, the at least one delivery address associated with the unique consumer identifier cannot be changed without causing the unique consumer identifier to be disabled" (claim 21). Final Rejection at 10. Nevertheless, the Examiner asserts that it would have been obvious to prevent a purchaser from changing the

delivery address in order to prevent intruders from tangling with the purchasing system in light of Edwards and Walker. *Id.* For the reasons discussed at length above, Edwards and Walker do not teach or suggest the features conceded to be missing from Egendorf.

Furthermore, Egendorf includes no motivation to include a purchaser identifier that is inextricably linked to at least one delivery address as is set forth in the claims, as amended. In fact, Egendorf teaches away from the present claims in so far as Egendorf teaches that during the course of making a purchase, the means of delivery of the goods or service will be established and the merchant may check with the provider that the shipping address supplied by the customer has been authorized. Egendorf, col. 4:3-12. This disclosure clearly shows (i) that the purchaser identifier, if any, in Egendorf is not inextricably linked to a pre-stored delivery address and (ii) that in the system of Egendorf a purchaser will have the opportunity to specify any delivery address that the purchaser desires at the time of purchase. Therefore, Egendorf's system will still be subject to potential fraudulent transactions made by thieves who have stolen the consumer's identifier. Thus, Egendorf teaches away from the system of the present claims and, therefore, contains no motivation to a person of skill in the art to modify Egendorf to include the features of claims 20-24.

With respect to the proposed combination of Egendorf with Lewis, Edwards, and Walker, Applicant refers to the arguments set forth above. Even if the proposed combinations are made, none of the references teaches or suggests the claimed feature of inextricably linking the delivery data to the purchaser identifier such that any change or attempted change to the delivery data will render the purchaser identifier inoperable, as well as other features highlighted above. For this reason, Applicant submits that claims 20-24 are allowable over the cited references.

C. SECONDARY CONSIDERATIONS WEIGH AGAINST A FINDING OF OBVIOUSNESS

1. **There Has Been A Long Felt, But Unresolved, Need In The Industry**

As set forth in Mr. Casper's declaration (attached hereto as Exhibit 1), credit card or debit card fraud, e.g., the theft and use of credit card and debit card numbers to make fraudulent purchases, has been an industry wide problem for both merchants and consumer for many years. Casper Dec. ¶4. Credit/debit card fraud costs cardholders and issuers hundreds of millions of dollars each year. Casper Dec. ¶5.

The emergence of the Internet and online purchasing has only exacerbated the problem of credit/debit card fraud, because the purchaser is not present at the point of sale and the merchant must rely solely on the credit/debit card number transmitted to its system. See, e.g., Casper Ex. 3 ("It's much easier to commit fraud online because you're not authenticating the buyer."). As such, credit/debit card fraudsters can use acquired numbers with virtual impunity. Casper Dec. ¶7. To date, despite attempts from credit card companies, banks, merchants, and even consumers, credit card fraud has grown in comparison to the rate of growth of e-commerce. Casper Dec. ¶8; Ex. 4, p. 1 ("While e-commerce has grown by nearly 74 percent in the past year, the amount of fraudulent transactions has grown even faster, jumping 114 percent."). Moreover, credit card fraud online accounts for 6.2 percent of all transactions, while such fraud in the normal "brick-and-mortar" world accounts for only about 1 percent. Id.

Part of the problem with online purchasing using a credit card is that the transmission of credits cards over the Internet to merchants is very susceptible to credit card number theft either at the source (i.e., from the consumer's personal computer), during transmission over the Internet, or from the Merchant who may or may not be trustworthy. By way of example, several large web sites have been hacked and credit cards numbers and other personal information stolen. Casper Dec. ¶9. Even the U.S. Department of The Navy has been hacked and had the credit card numbers stolen. Id.

Thus, the ability for fraudsters to acquire credits cards used freely on the Internet is one of the main problems plaguing e-commerce. In addition, credit card fraudsters are aided by the fact that current online purchasing systems permit the shipment of goods to any desired location. This creates an enormous loophole in many systems designed to prevent such fraud. Casper Dec. ¶13. The foregoing makes clear that the problem of credit card and debit card fraud has existed for a long period of time and is as of yet, despite many attempts, unresolved. Moreover, the ability of fraudsters to easily obtain credit card numbers freely used for online purchases and then have fraudulent purchases delivered to the location of the fraudster's choice has cost both consumers and merchants millions of dollars each year, and have stunted the growth of Internet e-commerce as discussed below. Casper Dec. ¶14-18.

The foregoing studies and news articles indicate two distinct, but related, problems with current online purchasing systems. First, because most present systems still require entry of the actual credit/debit card number into a web site form, the number is subject to being stolen by a hacker either from the consumer or the merchant's database. Thus, there is a need for a system that permits online purchases to be made without use of the actual credit/debit card number being entered and transmitted via the Internet to a merchant for authorization. Casper Dec. ¶19. Second, once a credit/debit card number or other code used to make online purchases is stolen, there are no mechanisms currently in place to reduce the ability of the fraudster to make successful fraudulent purchases with the stolen numbers or codes. This is because present systems permit the consumer to change the shipping address to any desired address. Thus, there is a need for a system that reduces a fraudster's ability to effectively use stolen purchasing numbers by linking the purchasing number to a pre-stored delivery address that cannot be changed. Casper Dec. ¶20.

2. **The Present Invention As Set Forth In Claims 1, 14, 17, 20, 22, and 25 Solves These Problems.**

Independent claims 1, 14, 17, 20, 22 and 25 of the present application solves both of the above problems by (1) reducing the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received, and (2) reducing the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only pre-stored delivery addresses. Casper Dec. ¶21. Thus, even if a consumer's unique consumer identifier for making purchases through the claimed system is stolen, the consumer identifier can only be used to make purchases that will be delivered to the pre-stored delivery addresses, thereby eliminating the thief's ability to make purchases and have the goods delivered to the location of the thief's choice. Id. The claimed invention, therefore, removes a major loophole in present systems, i.e., the ability to ship to any location. Id. at ¶22.

Moreover, as set forth in the claims of the present invention, the delivery address associated with a particular consumer identifier that has been compromised cannot be changed without disabling (e.g., rendering unusable) the consumer identifier that was compromised. This feature also frustrates the ability of thieves from using any acquired consumer identifiers. Casper Dec. ¶23.

Accordingly, the present invention as embodied in the claims comprises a system that combines a secure purchase processing system with the feature of permitting delivery of purchased goods to only pre-stored delivery address to thereby directly address the problem of online credit and debit card fraud and provides a solution thereto. Casper Dec. ¶24. The claimed system reduces the ability of thieves to both steal credit and debit card numbers and compromise

alternative consumer identifiers by permitting delivery of purchased goods to only to pre-stored delivery addresses. Id.

X. CONCLUSION

Applicant has made a diligent effort to place the Application in condition for allowance and respectfully submits that claims 1-6 and 8, 10, 12-25 in light of the amendments and arguments set forth above are in condition for immediate allowance. Consequently, if the Examiner cannot issue an immediate allowance of the present application, the Examiner is respectfully requested to contact the undersigned attorney to discuss the outstanding issues.

Applicant authorizes the U.S. Patent Office to charge any new and additional fees or charges, including any fees for a petition for an extension of time, to Deposit Account No. 19-4709, if necessary.

Respectfully submitted,

By: _____

Richard Eskew, Reg. No. 48,874
for Steven B. Pokotilow
Registration No. 26,405
Attorney For Applicant
Stroock & Stroock & Lavan LLP
180 Maiden Lane
New York, New York 10038-4982
(212) 806-5400

XI. APPENDIX

1. A processing system for processing a secure purchase order between a purchaser and a merchant across a public network, the processing system comprising:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least a purchaser identifier that is any alpha-numeric code generated by the processing system during account setup and being inextricably linked to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable for identifying a particular purchaser, payment data for effecting payment for purchased goods or services wherein the payment data is different from the purchaser identifier, and delivery data associated with said purchaser identifier, said delivery data including at least one delivery address of said purchaser for fulfillment of the purchase order;

a processor capable of communication with the purchaser account database via a private network and further capable of communication via a public network with a merchant system for receiving the purchase order, said purchase order including at least a monetary amount for a good and said purchaser identifier and not including the payment data which is not transmitted to the merchant;

wherein, in response to receipt of the purchase order including the purchaser identifier, the processor retrieves the payment data and the delivery data from the purchaser account database on the private network corresponding to the purchaser identifier, transmits the delivery data to the merchant to fulfill the purchase order, and uses the payment data to pay for the purchased goods or services without exposing the payment data to the merchant; and

wherein the merchant delivers the purchased goods or services to the purchaser using the delivery data.

2. The processing system of claim 1, wherein said delivery address is a physical address.

3. The processing system of claim 1, wherein said delivery address is an electronic address.

4. The processing system of claim 3, wherein said electronic address is an e-mail address.

5. The processing system of claim 1, wherein only one delivery address for a particular type of address is associated with the purchaser identifier.

6. The processing system of claim 1, wherein the disabler disables said purchaser identifier for a particular purchaser when either the purchaser identifier or the delivery data is altered.

7. (Canceled).

8. The processing system of claim 1, further comprising a securitizer disposed between a secure network and the public network; and

the secure network including the purchaser account database and the processor, and said securitizer preventing unauthorized access to said secure network.

9. The processing system of claim 8, wherein the disabler is operatively connected to said securitizer and said purchaser account information, said securitizer monitoring said processing system and determining if any alterations to said delivery data are being attempted and outputting a trigger to the disabler if said alterations are attempted, and the disabler disabling the particular purchase account information in response to the trigger.

10. The system of claim 9, wherein the disabler invalidates the purchaser identifier in response to the trigger.

11. (Canceled).

12. The processing system of claim 1, wherein the public network is the mail and the merchant is a catalog company.

13. The processing system of claim 1, wherein the merchant is a utility company.

14. A transaction processing service for facilitating the processing of a secure purchase order between a purchaser and a merchant across a public network, the processing service comprising:

a processing system, including:

a purchaser account database for storing therein purchaser account information for each purchaser, the purchaser account information including at least a purchaser identifier for identifying a particular purchaser and being generated by the processing system during account setup so as to be inextricably linked to a delivery address for use by the merchant to deliver a purchased good to the purchaser, and payment data for effectuating payment of the purchase order, and wherein the purchaser identifier is different than the payment data and cannot be used to make purchases except in connection with the transaction processing service;

the processing system being programmed to detect a change or attempted change in the delivery address linked to the purchaser identifier and, in response, render the purchaser identifier inoperable

wherein, in order to make a purchase, the purchaser accesses the merchant's electronic store system and selects one or more goods for purchase and transmits the purchaser identifier to the merchant, the merchant's electronic store system submits a purchase order and the purchaser identifier to the processing system, and, in response to receipt of the purchase order including the purchaser identifier, the processor retrieves the payment data and the delivery data from the purchaser account database on the private network corresponding to the purchaser identifier, transmits the delivery data to the merchant, and uses the payment data to pay for the purchased goods or services, and the merchant delivers the purchased goods or services to the purchaser using the delivery data; and

wherein the payment data is not transmitted by the purchaser to the merchant and the processing system pays for the purchased goods without exposing the payment data to the merchant.

15. The transaction processing service of claim 14, wherein said service is operated by a credit card company.

16. The transaction processing service of claim 14, wherein said service is operated by a financial institution.

17. A method of facilitating secure transactions between a purchaser and a merchant across a public network wherein, in order to make a purchase, the purchaser accesses a merchant electronic store system and selects one or more goods for purchase and transmits a purchaser identifier to the merchant electronic store system, and the merchant electronic store system generates a purchase order including the purchaser identifier, comprising the steps of:

storing purchaser account information which includes at least payment data for paying for purchased goods and delivery data for delivery of the purchased goods to the purchaser;

generating the purchaser identifier so that the purchaser identifier is inextricably linked to the stored delivery data, and wherein the purchaser identifier is any alpha-numeric code that is different from the payment data;

rendering the purchaser identifier inoperable in response to any change or attempted change in the stored delivery data;

receiving the purchase order including the purchaser identifier from the merchant electronic store system;

retrieving the delivery data and payment data associated with the received purchaser identifier;

effectuating payment for the purchased product using the payment data without exposing the payment data to the merchant; and

communicating only the delivery data for the purchaser identified by the purchaser identifier to the merchant.

18. The method of claim 17, wherein the method further comprises prior to the step of effectuating payment

determining whether the identified purchaser can pay for the purchased product; and

if said purchaser is not capable of paying, canceling the purchase order.

19. The method of claim 17, further comprising the step of invalidating the purchaser identifier if said delivery data is altered.

20. A method of facilitating secure transactions between purchasers and merchants across a public network, comprising the steps of:

at a purchaser system having access to a merchant store system:

selecting a product offered for sale by the merchant, the product being associated with a product identifier;

transmitting a purchaser identifier from the purchaser system to the merchant store system;

at the merchant store system:

receiving the purchaser identifier;

generating a purchase order for the selected product that includes the purchaser identifier; and

communicating the purchase order to the processing system; and

at the processing system:

processing the purchase order to retrieve delivery data and payment data associated with the purchaser identifier;

wherein the purchaser identifier is any alpha-numeric code that is different from the payment data, and the purchaser identifier is inextricably linked to the delivery data such that if the delivery data is changed or attempted to be changed the purchaser identifier will be rendered unusable;

effectuating payment for the selected product without exposing the payment data to the merchant; and

communicating the delivery data corresponding to the purchaser identifier to the merchant.

21. The method of claim 20, wherein said purchaser is not given an opportunity to change said delivery data.

22. A purchasing system for facilitating secure electronic transactions between a consumer and a merchant, wherein a secure consumer account is stored on the purchasing system and the account includes consumer payment information and at least one delivery address for delivering purchased items; the purchasing system comprising:

a communication connection to a merchant system via a network;

a server system operative with programming to:

receive a request for payment from the merchant system in response to an order placed by the consumer with the merchant to purchase items, wherein the request for payment includes a unique consumer identifier unrelated to the consumer payment information which is associated with the secure consumer account;

retrieve the consumer payment information from the consumer account associated with the unique consumer identifier and effectuate payment for the order to the merchant;

retrieve the delivery address from the consumer account associated with the unique consumer identifier and transmit the delivery address to the merchant computer for delivery of the purchased item; and

wherein once the secure consumer account is established by the consumer and the unique consumer identifier is assigned to the consumer account, the at least one delivery address associated with the unique consumer identifier cannot be changed without causing the unique consumer identifier to be disabled.

23. The system of claim 22, wherein if the delivery address is changed and the unique consumer identifier is disabled, the consumer must be issued a new unique consumer identifier prior to making a purchase using the secure consumer account stored on the purchasing system.

24. The system of claim 22, wherein only a single delivery address is stored in the secure consumer account, such that purchased items can only be delivered to the single delivery address.

25. A processing system for processing a secure purchase order between a purchaser and a merchant across a public network, the processing system comprising:

a processing system residing on a private network and in communication with a purchaser computer and a merchant computer via a public network;

a purchaser account database in communication with the processing system via the private network;

the processing system programmed to:

receive from the purchaser computer purchaser account information including at least delivery data including at least one delivery address for the purchaser and payment data for effecting payment of purchased goods or services;

store the purchaser account information on the purchaser account database;

generate a purchaser identifier that is an alpha-numeric code having no monetary value and that is unrelated to any personally identifiable information of the purchaser; and

link the purchaser identifier to the delivery data such that any change or attempted change to the delivery data will render the purchaser identifier inoperable; and

in order to process a purchase order from the purchaser, the processing system further programmed to:

receive the purchase order, including order information and the purchaser identifier;

verify the purchaser identifier and retrieve the payment data and the delivery data corresponding to the purchaser identifier from the purchaser account database;

arrange for payment to be made to the merchant for the purchased goods or services without exposing the payment data to the merchant; and

transmit only the delivery data and a payment authorization to the merchant to fulfill the purchase order, whereby the purchaser need not enter or transmit the payment data at any time to make a purchase.

EXHIBIT 1

UNITED STATES PATENT & TRADEMARK OFFICE

Application No.	:	09/521,636
Title	:	SECURE TRANSACTION PROCESSING SYSTEM AND METHOD
Applicant	:	Andrew Casper
Filed	:	March 8, 2000
TC/AU	:	3628
Examiner	:	Frantzy Poinvil
Docket No.	:	105026/0002

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

DECLARATION OF ANDREW CASPER

UNDER 37 C.F.R. SECTION 1.132

Certificate of Mailing (37 C.F.R. 1.8)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450, on January 12, 2004.

Typed or printed name of person signing this certificate:

Richard Esdew

Signature

1. I am the sole inventor of the above-referenced patent application for a Secure Transaction Processing System filed on March 8, 2000 and claiming priority to Provisional Patent Application Serial No. 60/157,774 filed on October 5, 1999.

2. I am making this Declaration in support of a concurrently filed Amendment in response to the outstanding Office Action of August 14, 2003 in which the Examiner rejected all of the claims pending in the present application. I have reviewed the rejections made by the Examiner, including the cited references and the Examiner's rationales in making the rejections.

3. This Declaration and the attached exhibits describe and evidence the non-obviousness of the claimed invention, and, in particular, set forth the long-felt, but unresolved, need in the relevant on-line purchasing industry for a system that adequately counteracts theft and use of sensitive financial information to make fraudulent purchases over the Internet and other networks. Furthermore, this Declaration and the attached exhibits show the nexus of the claimed invention to solving this long-felt, but unresolved, need in the on-line purchasing industry.

CREDIT CARD/DEBIT CARD FRAUD IS A LONG STANDING PROBLEM

4. Credit card or debit card fraud, e.g., the theft and use of credit card and debit card numbers to make fraudulent purchases, has been an industry wide problem for both merchants and consumer for many years. For instance, on Visa's web site, a summary of the history of Visa U.S.A. notes that, in 1984, "the rapid growth of the payment card industry in mid-80s leads to a rise in credit card fraud and counterfeiting." See Exhibit 1, p. 2.

5. In an August 1997 publication of the Federal Trade Commission ("FTC"), Bureau of the Consumer Protection, Office of Consumer and Business Education, the FTC outlined

various facts to help consumers guard against credit card fraud. See Exhibit 2. In the publication, the FTC noted that credit and charge card fraud cost cardholders and issuers hundreds of millions of dollars each year. See id. at p. 2.

6. Because merchants often suffer the most from credit/debit card fraud in the form of "charge-backs", merchants have banded together to form several consortiums to combat credit/debit card fraud. Once such group that I am aware of is Merchant 911, which can be found at http://www.merchant911.org.

E-COMMERCE COMPLICATES CREDIT/DEBIT CARD FRAUD PROBLEM

7. The emergence of the Internet and online purchasing has only exacerbated the problem of credit/debit card fraud, because the purchaser is not present at the point of sale and the merchant must rely solely on the credit/debit card number transmitted to its system. See Exhibit 3 ("It's much easier to commit fraud online because you're not authenticating the buyer."). As such, credit/debit card fraudsters can use acquired numbers with virtual impunity.

8. To date, despite attempts from credit card companies, banks, merchants, and even consumers, credit card fraud has grown in comparison to the rate of growth of e-commerce. See Exhibit 4, p. 1 ("While e-commerce has grown by nearly 74 percent in the past year, the amount of fraudulent transactions has grown even faster, jumping 114 percent."). Moreover, credit card fraud online accounts for 6.2 percent of all transactions, while such fraud in the normal "brick-and-mortar" world accounts for only about 1 percent. See Exhibit 5, p. 2.

9. Part of the problem with online purchasing using a credit card is that the transmission of credits cards over the Internet to merchants is very susceptible to credit card number theft either at the source (i.e., from the consumer's personal computer), during transmission over the Internet, or from the Merchant who may or may not be trustworthy. By way of example, several large web sites have been hacked and credit cards numbers and other

personal information stolen. See Exhibit 6, p. 2-3. Even the U.S. Department of The Navy has been hacked and had the credit card numbers stolen. See Exhibit 7.

10. In a more recent FTC publication from March 2003, the FTC issued a notice directed specifically at the problem of online credit and debit card fraud as it pertained to the use of electronic payments over the Internet. See Exhibit 8. The FTC recognized that using present systems fraud on the Internet could not be controlled. See id. at p. 3.

11. In a September 2003 FTC report on identity theft, which includes credit/debit card fraud, a survey indicated that it sometimes takes weeks, if not months, for consumers to detect fraud. See Exhibit 9, p. 8. In the case of credit card fraud, according to the survey, it took 61% of consumers longer than one week to recognize the fraud. Id. Of those 61% of consumers, 33% of consumers did not recognize the fraud until after at least one month had passed. Id.

12. Another article from U.S. News.com again recognized the problem of credit card fraud over the Internet. See Exhibit 10. In a statement from Susan Grant, Director of the National Fraud Information Center in Washington, the problem of credit fraud on the internet comes into focus: "no matter how somebody might get a hold of consumer's financial information, the ability to use it on the Internet is huge." Id. at p. 2.

13. Thus, the ability for fraudsters to acquire credits cards used freely on the Internet is one of the main problems plaguing e-commerce. In addition, credit card fraudsters are aided by the fact that current online purchasing systems permit the shipment of goods to any desired location. This creates an enormous loophole in many systems designed to prevent such fraud.

14. The foregoing makes clear that the problem of credit card and debit card fraud has existed for a long period of time and is as of yet, despite many attempts, unresolved. Moreover, the ability of fraudsters to easily obtain credit card numbers freely used for online purchases and then have fraudulent purchases delivered to the location of the fraudster's choice has cost both consumers and merchants millions of dollars each year, and have stunted the growth of Internet

e-commerce as discussed below. See Exhibit 11, p. 2 (Ex. 11 also lists many other articles showing the need for a solution to the problem of online credit/debit card fraud).

ONLINE CREDIT/DEBIT CARD FRAUD HAS HINDERED THE EXPANSION OF E-COMMERCE.

15. In a June 21, 2001 survey by Jupiter Media Metrics, consumers said that they believed their credit card was 12 times more likely to be defrauded on-line than off-line, even though actual data suggested that the occurrence of on-line fraud was just 3 or 4 times that of off-line fraud. See Exhibit 12. Moreover, most internet consumers desire an alternative to having to use their credit card to make online purchases, thus highlighting the need for a solution such as my invention. See Exhibit 13.

16. Despite some recent successes, I believe that online purchasing is being hampered by both the perception and realities of credit/debit card fraud.

17. These trends have not gone unnoticed by major banks and credit card companies, and such companies have taken measures to combat or reduce the risks associated with on-line purchasing. For example, Visa launched its "Next Card" program in 2001 to help consumers protect against someone stealing their personal data. See Exhibit 14. This attempted solution, like many other Internet solutions, focused on encryption techniques for preventing the theft of credit card numbers as they were transmitted over the Internet. Ultimately, however, even Visa recognized that "it is impossible to guarantee that an Internet thief will never get your Next Card Visa number". See id. at p. 3. Visa, like other banks and credit card companies, still did not provide a system that would provide disincentives to using stolen credit card numbers. Thus, the only way for Visa to truly provide a solution to the credit card fraud problem was to guarantee that it would cover the full cost of any fraud against the consumer's account that might arise from fraudulent usage of the next card Visa over the Internet. See id. The Visa solution, therefore, was a downstream and ultimately unsatisfactory solution to the problem for merchants who oftentimes get stuck paying for fraudulent purchases.

18. Visa later introduced a new system referred to as the "Verified by Visa" system. This system simply links a password to a credit card number. The user is still required to transmit both their credit card number and password over the Internet to potentially untrustworthy merchants. See Exhibit 15.

TWO MAIN PROBLEMS TO BE SOLVED

19. The foregoing studies and news articles indicate two distinct, but related, problems with current online purchasing systems. First, because most present systems still require entry of the actual credit/debit card number into a web site form, the number is subject to being stolen by a hacker either from the consumer or the merchant's database. Thus, there is a need for a system that permits online purchases to be made without use of the actual credit/debit card number being entered and transmitted via the Internet to a merchant for authorization.

20. Second, once a credit/debit card number or other code used to make online purchases is stolen, there are no mechanisms currently in place to reduce the ability of the fraudster to make successful fraudulent purchases with the stolen numbers or codes. This is because present systems permit the consumer to change the shipping address to any desired address. Thus, there is a need for a system that reduces a fraudster's ability to effectively use stolen purchasing numbers by linking the purchasing number to a pre-stored delivery address that cannot be changed.

MY INVENTION SOLVES BOTH OF THESE PROBLEMS

21. My invention as set forth in the claims of the present application solves both of the above problems by (1) reducing the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received, and (2) reducing the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only prestored delivery

addresses. Thus, even if a consumer's unique consumer identifier for making purchases through the claimed system is stolen, the consumer identifier can only be used to make purchases that will be delivered to the prestored delivery addresses, thereby eliminating the thief's ability to make purchases and have the goods delivered to the location of the thief's choice.

22. The claimed invention, therefore, removes a major loophole in present systems, i.e., the ability to ship to any location.

23. Moreover, as set forth in the claims of the present invention, the delivery address associated with a particular consumer identifier that has been compromised cannot be changed without disabling (e.g., rendering unusable) the consumer identifier that was compromised. This feature also frustrates the ability of thieves from using any acquired consumer identifiers.

24. Accordingly, the present invention as embodied in the claims comprises a system that combines a secure purchase processing system with the feature of permitting delivery of purchased goods to only pre-stored delivery address to thereby directly address the problem of online credit and debit card fraud and provides a solution thereto. The claimed system reduces the ability of thieves to both steal credit and debit card numbers and compromise alternative consumer identifiers by permitting delivery of purchased goods to only to prestored delivery addresses. Thus, I believe that my invention has a direct nexus to the long-felt need for a solution to the problem of fraudulent online credit and debit card purchases.

THE REFERENCES CITED BY THE EXAMINER DO NOT TEACH OR SUGGEST SUCH A SYSTEM

25. The references cited by the Examiner, namely the Lewis (U.S. Patent No. 6,233,565) and Egendorf (U.S. Patent No. 6,188,994) references, do not teach or suggest the claimed system.

26. Specifically, the Lewis reference does not teache a secure processing system that processes purchase requests without exposing payment information (e.g., credit/debit card numbers) to merchants and the feature of inextricably linking the consumer identifier to pre-

stored delivery addresses and rendering the consumer identifier inoperable in response to any change or attempted change to the delivery data as set forth in the claims as presently amended. Moreover, Lewis states that "after authentication is completed, the user then purchases the ultimate goods or services, postage in the case of the preferred embodiment, utilizing credit cards, ACH debit cards or checks as the method of payment, and electronically confirming the sale." Lewis, col. 3, lines 15-19. Thus, Lewis fails to teach or suggest a feature of the claims of the present application, namely the feature of using the payment data to pay for the purchased goods or services ***without exposing the payment data to the merchant***.

27. Similarly, the Egendorf does not teach or suggest a system that combines a secure purchase processing system with a consumer identifier that can be used to make purchases online and that is inextricably linked to pre-stored delivery addresses that cannot be changed without rendering the consumer identifier unusable. Further, Egendorf teaches specifying the means of delivery of the goods or services during the course of making a purchase. Thus, Egendorf fails to teach or suggest a feature of the claims of the present application, namely the feature of permitting delivery only to pre-stored delivery addresses.

28. Moreover, the Examiner fails to point to any motivation in either Lewis or Egendorf to suggest modifying those references to include the claimed features. The Examiner argues in the outstanding Office Action that the desire in Lewis to prevent fraud renders the claimed fraud prevention solution of combining secure purchase processing system that does not expose sensitive payment information with a consumer identifier inextricably linked to prestored delivery addresses such that to purchased good or services can only be delivered to the selected prestored delivery address. However, Lewis simply does not teach or even suggest these features and the Examiner's obviousness rejection amounts to a reconstruction of the Lewis reference in light of my disclosure. I am advised that such hindsight reconstruction is impermissible as a basis of a rejection.

29. Based on these differences between the cited references and the long-felt, but unresolved, need in the industry for a system that both (1) reduces the risk that a credit number might be stolen or compromised by creating a secure third party entity to hold consumer's credit cards and deliver only purchase authorizations and pre-stored delivery addresses to merchants when a purchase request is received and (2) reduces the ability of a thief to use a stolen consumer identifier, such as a pin number, by limiting delivery of the purchased goods or services to only pre-stored delivery addresses, I believe that my invention as embodied in the claims of the present application are non-obvious over the cited references and are therefore allowable.

30. I further declare that all statements made herein are of my own knowledge and are true and that all statements made on information and belief and believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Date: January 8, 2004

Andrew Casper

Exhibit 1

Who We Are

A Legacy of Payment
Anytime, Anywhere, Anyway
It's hard to believe that the payments industry is just a little over 40 years old. Just think back to the days when consumers and merchants had only two choices — cash and checks. Visa has had a fundamental impact on the evolution of payments, how consumers choose to pay and how merchants choose to be paid.

Visa traces its history back to 1958 when Bank of America launched its blue, white and gold BankAmericard in California. In 1970, an association, National BankAmericard, Inc., was formed of those U.S. banks issuing BankAmericards. In 1974, Bank of America's international licensees chartered an international company, IBANCO, to administer BankAmericard, Inc. outside the U.S. In 1976, IBANCO became Visa International and National BankAmericard, Inc. became Visa U.S.A. Take a look back at our history.

1958
Bank of America based in San Francisco, California, issues BankAmericard. With the entire state of California as its market, the card is an early success, and it is the first "revolving-credit" card with universal merchant acceptance, allowing cardholders the option of paying their account balance in installments with a monthly finance charge applied to the remaining balance.

1966
Bank of America expands its bankcard program by forming the BankAmericard Service Corporation, licensing banks outside of California to issue cards to their customers. Because the cost of bankcard programs is shared among its Member financial institutions, even small banks across the country are able to join. The Interbank Card Association, which later becomes Master Charge, is formed.

1969
Most regional banks convert their independent programs to either BankAmericard or Master Charge.

1970
BankAmericard transfers control and ownership of the BankAmericard program to the banks that issue the cards, forming National BankAmericard Inc. (NBI). At this time, more than 1,400 banks offer either BankAmerica or Master Charge credit cards.

1973
NBI pioneers e-commerce and introduces the world's first global electronic card authorization system, BASE I, reducing the time consumers need to wait to have their transactions authorized from more than five minutes to less than one minute. And authorization is now available 24 hours a day.

1974
International Bankcard Company (IBANCO) is formed to administer the

BankAmericard program internationally. The card encounters some resistance because its name is identified too closely with the U.S. and the Bank of America. The same year, "Base II" is introduced, the first electronic clearing and settlement system, making it possible for merchants to transmit authorized transactions electronically, greatly reducing paper work and significantly speeding up the transaction process.

1975
NBI introduces the first national deposit access card, enabling cardholders to debit charges from their deposit account rather than having the charge posted to a line of credit.

1976
BankAmericard changes its name to Visa, a simple, memorable name with an international flavor that is pronounced the same way in almost every language. NBI is renamed Visa U.S.A. and IBANCO is changed to Visa International.

1979
Visa introduces the first electronic dial terminal at the point of sale, which allows for much speedier purchase transactions. This leads the way to electronic data capture (EDC) point-of-sale terminals, which virtually eliminate the time-consuming process of paper deposits.

1982
Visa issues the first premium card — Visa Premier — to provide new kinds of services for upscale customers.

1983
Building on its anytime, anywhere promise, Visa launches the world's first global ATM network, providing 24-hour cash access to cardholders around the world and contributing to the convenience of modern business and leisure travel.

1984
The rapid growth of the payment card industry in the mid-80s leads to a rise in credit card fraud and counterfeiting. Visa establishes the Visa Risk Identification Service, the first computer-based system to pinpoint suspicious card transactions at merchant locations.

1985-1988
Visa sales volume doubles.

1986
Globally, Visa becomes the first payment card system to offer multiple-currency clearing and settlement, providing financial institutions with faster methods of restitution and greatly increasing the efficiency of international transactions. Today's Visa network is capable of processing payment transactions in 160 different currencies.

1987
Visa establishes the first computerized card transaction processing network in China.

1988
Visa Member issues the first bankcard in Russia.

1993
Visa is the first to apply state-of-the-art neural network technologies to payments, thus greatly reducing the incidence of card fraud by giving Visa Member banks smarter and timelier data about suspicious transactions. By analyzing typical card usage patterns, the neural

network-based risk management tool invented by Visa immediately notifies banks so they can inform their customers if a card appears to have been used by someone other than the legitimate cardholder. Visa offers the first international pre-paid card, Visa Travel Money. This allows travelers to put a set amount of money on their card in one currency and access that account while traveling in other countries, enhancing the safety and convenience of international travel and currency exchanges. Visa issues the first smart card that allows cardholders to accumulate merchant loyalty points by making purchases on their payment cards. Visa becomes the first to offer a suite of corporate, business and purchasing cards to accommodate the needs of business of all sizes.

1995
Visa co-develops industry-wide chip card specifications, Europay/Visa/MasterCard (EVM), to ensure that all chip cards will operate with all chip-reading terminals, regardless of location, financial institution, or manufacturer. As a result, smart credit cards and debit cards are now standardized to the point where cardholders can confidently use their chip cards to access their accounts from any EMV terminal worldwide.

1997
The first SET 1.0 (Secure Electronic Transaction) purchase using a smart card is completed. This technology, co-developed by Visa, provides a high level of privacy, security, and authentication for payment card transactions made over the Internet. Visa announces the prototype for the first contactless commuter-cash smart card. Contactless terminals do not need a card to be physically inserted into the terminal and offer greater convenience and flexibility to cardholders.

1998
Visa, together with Standard Chartered Bank, introduces the world's first multi-application smart card based on open standards-based technology. As a result, it becomes more cost-effective for banks to offer multi-application cards that enable consumers to access multiple financial accounts and other types of services - all on a single card. For example, debit accounts, lines of credit, prepaid accounts as well as secure Internet shopping or merchant loyalty programs can now all be stored on one card.

1999
Globally, Visa becomes the first to process 25 billion consumer payment transactions per year. Visa is the first payment association to promote a global infrastructure for smart cards across multiple industries as a founding member of GlobalPlatform, Inc. Visa conducts the world's first euro transaction using a payment card in the European Union. Visa joins the Wireless Application Protocol (WAP) Forum to develop standards for wireless delivery. Visa completes the first download of electronic cash via mobile phone that are powered by the GSM (Global Systems and Mobile Phone) network in Leeds, UK. Visa announces a pilot program with Nokia and MeritaNordbanken of Finland enabling cardless payments via mobile phones at both physical merchants and on the Internet. Visa, together with Citibank and the General Services Administration, introduces the world's most sophisticated, multi-application smart card. It is the first smart card to combine credit, employee identification, access control and biometric verification.

2000
Visa reaches a key milestone with one billion cards in use. Visa announces an enhanced Consumer Zero Liability Policy, which was originally launched in 1997. The new rule virtually eliminates consumer liability in cases of Visa card fraud over the Visa system, including Internet transactions. Under the previous policy, cardholders could be

held liable for up to $50 if their credit or debit cards were fraudulently used on the Visa system, and they failed to report theft or unauthorized use within two business days. The new policy does not cover commercial card transactions. On April 3, 2000 Visa International moved its systems and processing services division into a wholly owned subsidiary company, named Inovant (www.inovant.com). Inovant provides global transaction processing for Visa. smart Visa, a multi-function chip product, is launched in the United States. Visa Buxx is launched to open an underserved market of teenaged consumers and offer parents a tool to teach their teens about responsible money management. Visa U.S.A. announces Direct Exchange, which paves the way for a new generation of payment capabilities. Holiday spending volume on Visa credit and check cards between November 24 and December 29, 2000, reaches $101 billion. Online spending more than doubles over the past year. Visa U.S.A. launches it's national consumer education program, Practical Money Skills for Life which is aimed at helping high school students learn better money management skills.

2001

Visa completes the world's first secure payment transaction using a Palm™ handheld computer. Palm and Visa have worked with terminal manufacturers Ingenico and VeriFone to enable the secure transfer of payment information from a Palm handheld to a VeriFone or Ingenico point of sale payment terminal using infrared technology. smart Visa Business cards, chip-enabled payment products tailored to the small business market, are launched in the United States.

Exhibit 2

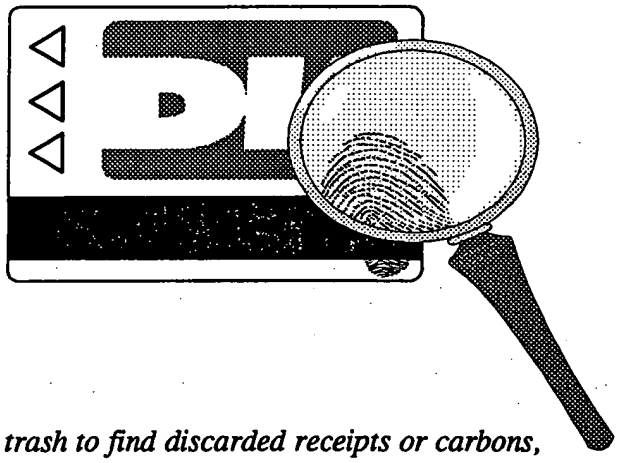
CREDIT

FOR THE CONSUMER www.ftc.gov

FEDERAL TRADE COMMISSION 1-877-FTC-HELP

FTC FACTS for Consumers

Avoiding Credit and Charge Card Fraud



A thief goes through trash to find discarded receipts or carbons, and then uses your account numbers illegally.

A dishonest clerk makes an extra imprint from your credit or charge card and uses it to make personal charges.

You respond to a mailing asking you to call a long distance number for a free trip or bargain-priced travel package. You're told you must join a travel club first and you're asked for your account number so you can be billed. The catch! Charges you didn't make are added to your bill, and you never get your trip.

Credit and charge card fraud costs cardholders and issuers hundreds of millions of dollars each year. While theft is the most obvious form of fraud, it can occur in other ways. For example, someone may use your card number without your knowledge.

It's not always possible to prevent credit or charge card fraud from happening. But there are a few steps you can take to make it more difficult for a crook to capture your card or card numbers and minimize the possibility.

Guarding Against Fraud

Here are some tips to help protect yourself from credit and charge card fraud.

Do:

- Sign your cards as soon as they arrive.
- Carry your cards separately from your wallet, in a zippered compartment, a business card holder, or another small pouch.
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep an eye on your card during the transaction, and get it back as quickly as possible.
- Void incorrect receipts.
- Destroy carbons.
- Save receipts to compare with billing statements.
- Open bills promptly and reconcile accounts monthly, just as you would your checking account.
- Report any questionable charges promptly and in writing to the card issuer.
- Notify card companies in advance of a change in address.

Don't:

- Lend your card(s) to anyone.
- Leave cards or receipts lying around.
- Sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total.
- Write your account number on a postcard or the outside of an envelope.
- Give out your account number over the phone unless you're making the call to a company you know is reputable. If you have questions about a company, check it out with your local consumer protection office or Better Business Bureau.

Reporting Losses and Fraud

If you lose your credit or charge cards or if you realize they've been lost or stolen, immediately call the issuer(s). Many companies have toll-free numbers and 24-hour service to deal with such emergencies. By law, once you report the loss or theft, you have no further responsibility for unauthorized charges. In any event, your maximum liability under federal law is $50 per card.

If you suspect fraud, you may be asked to sign a statement under oath that you did not make the purchase(s) in question.

For More Information

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION
1-877-FTC-HELP www.ftc.gov

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education

August 1997

Exhibit 3

Enterprise software

Study says online fraud saps sales

Last modified: March 4, 2002, 6:55 AM PST

By Margaret Kane
Staff Writer

PRINT EMAIL SAVE

Merchants lose a higher percentage of sales to fraud online than offline, according to a new report from GartnerG2.

Merchants surveyed by GartnerG2, a service from research firm Gartner, reported that they lost 1.14 percent of all online sales to fraud in 2001, or about $700 million. During that same time period, Visa International and MasterCard reported that about .06 percent of physical world sales were lost to fraud, said Avivah Litan, research director at GartnerG2.

"There's a lot more sales going on in physical world, but relative percentages are much higher," she said. "It's just much more relative pain for the merchant."

Fraud rates were up only slightly from 2000, when merchants reported 1.13 percent, but merchants said the problem was becoming more difficult to deal with, Litan said.

Merchants were rejecting around 5 percent of Internet transactions, on average, as "suspicious," Litan said. And at large retailers that sell more than 25 percent of their goods and services online, the figure was up to 7 percent.

"It's much easier to commit fraud online because you're not authenticating the buyer. You don't have someone walking into a store and signing receipt," Litan said, adding that there are programs out there that can enter fake numbers, without even a person behind them.

Credit card companies and merchants have been trying to fight back. Visa launched its Verified by Visa program last year, which allows merchants to prompt shoppers for a password to verify their identity. MasterCard, meanwhile supports two programs, the Universal Cardholder Authentication Field standard and Secure Payment Application, designed to authenticate online consumers.

GetUptoSpeed

ENTERPRISE SECURITY | VOIP
OPEN SOURCE | WEB SE
UTILITY COMPUTING | WI-FI

Dose of utility comp
HP's Mark Linesch s computing can ease companies' pain, but overnight.
PLAY AUDIO
▸ Utility computing

▸ CNET's audiocast a

Security 2004
Enterprise Strategy G Oltsik says security w a hot topic this year, particular notes will b

▸ Enterprise security

Open source under microscope
University researche Scacchi and colleagu

examine phenomena
community building.
‣ Open source

Metaphysics of VoIP
Policy analyst Rando
says the future of Vo
on how regulators cla
‣ VoIP

TRACK THE PLAYERS
Ten Java software companies, includ
get behind an effort aimed at making
easier to use.
‣ Web services

‣ **This week's headlines**

Latest headlines

- Apple continues modest move into c
- Gadgets have Macworld spotlight
- IT buyers lay out new plans for 2004
- D-Link inks deal to bring Radio@AO
- Red Hat settles font lawsuit
- Scientists team up for nanotube brea
- IDC to RFID: Tags, you're it
- Rivals may not fight in Dell's switch w
- ATI puts 3D graphics in cell phones
- Sony downplays PS2 launch in Chin
- Toshiba spotlights high-definition DV
- BT lures consumers with free Wi-Fi
- Napster fills in the blanks with CD de
- Motorola banks on new gadgets, fea
- Study: Wi-Fi weaving its way into ho

Most popular headline

- Gadgets have Macworld spotlight
- Apple unveils smaller iPod, new soft
- Microsoft readies new Mac Office
- Open-source databases gaining favo
- Microsoft abandons Smart Display e
- Computing giants to debut new gear
- Year in review: News.com special re
- Happy New Worm
- The duel of the dual-layer DVD form
- Writing an end to the bio of BIOS

CNET NEWSLETTERS
CLICK ON A TITLE BELOW TO LEARN

☐ News.com Morning Dispatch sample
☐ News.com Afternoon Dispatch sample

Exhibit 4

Enterprise software

VeriSign tracks buyers to fight e-fraud

Last modified: June 18, 2003, 3:28 PM PDT

By Robert Lemos
Staff Writer, CNET News.com

In a bid to beat Internet fraud, VeriSign is introducing a service for merchants that will compare credit card numbers, the names of cardholders and the Net address of buyers to spot scams.

The Internet services company announced on Wednesday a new Fraud Protection Service that ties geographical information from its domain registry database--which is managed by VeriSign's Network Solutions--to timing data from its credit card clearinghouse service. The technology, which the company has tested during the last 18 months on its own business, will identify transactions that have an unacceptable probability of being fraudulent.

"It is no secret that Internet commerce is hot again," said Stratton Sclavos, chairman and CEO of VeriSign. "The bad news is that it has become a very big target. As we have seen a shift in the economy, we have seen a shift in the rate of crime."

While e-commerce has grown by nearly 74 percent in the past year, the amount of fraudulent transactions has grown even faster, jumping 114 percent, Sclavos said. Combining Network Solutions geolocational data with data on the timing of online credit card transactions has worked to reduce fraud rates, he said.

The Fraud Protection Service matches up credit card numbers, the names of cardholders and the Internet addresses of the transaction originations in order to estimate validity. "We correlate all that together, and we make inductive decisions about whether that transaction is fraudulent," Sclavos said.

For example, if the service detects that a U.S. citizen's transaction is actually coming from Russia--based on the buyer's Internet address--the confidence that the transaction is valid would plummet.

"With very little learning, just by flipping the switch, we think it will recognize 50 percent of the fraud on a merchant's system," Sclavos said.

Currently, one in four computers and software packages is bought

online, and one out of every eight books is bought online, Allan Trosclair, executive director of the Coalition for the Prevention of Economic Crime, said during a conference call with VeriSign.

"As (VeriSign) moves this product onto the market, I think we will see a reduction in the amount of fraud," Trosclair said.

The service, targeted at Web retailers, is the latest in a recent series of security offerings from VeriSign.

Earlier this month, the Mountain View, Calif., company signed a deal with Microsoft to integrate its digital authentication technology with Microsoft's newest version of its server operating system, Windows Server 2003.

The technology, which uses a variant of the mathematics behind encryption, lets people digitally sign data and verify their identity online. VeriSign, which makes server software that manages such signatures on a large scale, plans to launch a service that will take advantage of new features in Windows Server 2003. By working together, Microsoft and VeriSign hope to make authenticated Web services easier to use and more likely to interoperate.

In addition, VeriSign gained Merrill Lynch as a client for its new security monitoring services in late May. The company will electronically watch the computer systems of the giant investment bank and financial management company and work to prevent attacks and intrusions. The company will also be responsible for keeping Merrill Lynch's 300 computer-security devices up to date, it has said.

The fraud protection costs $19.95 a month and five cents a transaction for the basic service, which includes U.S. processing. Merchants are charged a fee of $49.95 a month and 10 cents a transaction for the enhanced service, which accepts international transactions. The service also works in conjunction with the secure transaction services from Verified by Visa and Mastercard SecureCode, according to statements by VeriSign.

Dan Moniz, staff technologist for the Electronic Frontier Foundation (EFF), worried that the service signaled the latest move by a company to offer technology that eroded the anonymity of the Internet.

"It will make anonymous transactions that much harder in the name of reducing the number of chargebacks," he said, referring to refunds made typically at the merchant's expense. "Do you start blocking people because they don't want to identify themselves?"

In the end, people that want to buy digital goods anonymously might have to subscribe to a special service and pay extra, he said.

Related stories

- Microsoft, VeriSign ink security deal
  June 2, 2003
- VeriSign grabs Merrill Lynch deal
  May 21, 2003

- MasterCard tests high-tech payments
  December 13, 2002
- **Get this story's "Big Picture"**

Related quotes

Quotes delayed 20+ minutes
▼ VeriSign Inc **VRSN** 17.33 -0.57 (-3.18%)

White papers about Authentication More results
- Managed Security Services Overview
  Cisco Systems
- Security Intelligence & Control Services
  VeriSign
- Security Intelligence and Control Services
  VeriSign

Videos about Authentication , Auctions More videos
Would you like Wi-Fi with that?
Dave Vucina, CEO, Wayport

Exhibit 5

Security

Study: Thriving Internet blighted by bugs

Last modified: October 13, 2003, 11:45 AM PDT

By Robert Lemos
Staff Writer, CNET News.com

Internet usage has jumped in the last year, but digital threats--such as junk e-mail and e-commerce fraud--continue to overshadow those gains, VeriSign announced on Monday.

Several measures of network traffic show an increase, according to a survey by VeriSign that looked at data generated by its Internet operations.

The number of queries to VeriSign's domain name service (DNS) system--the address books of the Internet--during the first week of the month of August increased 50 percent over the same period the previous year, while DNS lookups for e-mail grew 245 percent, the company found.

Unsolicited bulk e-mail--or spam--accounted for most of that boost, said Ken Silva, vice president of information security for VeriSign.

"The number of Internet uses or activity does continue to grow, but the dangerous activity on the Internet is growing faster than that," he said. "In August, we saw an incredible rise in the number of incidents, mainly due to security incidents."

Get Up to Speed on...
Enterprise security ▸
Get the latest headlines and company-specific news in our expanded GUTS section.

VeriSign has a unique view of the Internet because it has a role in so many aspects of the functions of the Net. The Mountain View, Calif.-based company maintains the registry databases for the .com and .net top-level domains. Its subsidiary, Network Solutions, is a registrar, which means it provides a service to let people reserve domain names.

The security company also offers digital-signature services for Web sites and enterprises, to help them heighten the security of e-commerce and business-to-business transactions. It has another e-commerce service: Credit-card processing.

VeriSign says it has been collecting the data for the past year. It released a snapshot of its analysis in its Internet Security Intelligence Briefing on Monday.

The company reported that e-commerce transactions in the second quarter of 2003 rose 17 percent per merchant this year, on average, compared with the same period the previous year. However, fraud on the Internet continued to grow, accounting for 6.2 percent of all transactions--far more than the 1 percent that is normal in the brick-and-mortar world, Silva said.

"There is a surprisingly high correlation between the IP (Internet protocol) source addresses of fraudulent activity and other hacker activity," he said.

As for the security events detected by devices VeriSign manages, the number of those jumped 99 percent in August, compared with the totals for May. The United States appears to be the leading source of such attacks, accounting for nearly 81 percent of the incidents.

However, two significant computer worms and a serious virus incident hit the Internet during August and may have accounted for part of the dramatic increase.

That month saw the MSBlast worm and a variant of that program spread to more than a million computers, security company Symantec has estimated. In addition, the computer virus SoBig.F spread to a projected tens of thousands of computers worldwide, producing an avalanche of spam as it attempted to infect more computers. In sending those messages, the SoBig.F worm caused the number of DNS queries related to e-mail to increase to 10 to 25 times the average, according to VeriSign's data.

The company is touting such insights into the data as part of a new family of security services, called the Security Intelligence and Control Services.

"Most people think if they buy the tools, such as intrusion-detection (software) and firewalls--they think they are covered. That's not necessarily true," Silva said. "Don't just sit in the foxhole. (You need to) see things as they happen around the world in a real-time fashion."

Dig deeper: Networking | Security

Related stories

- VeriSign changes tactics on security
  October 7, 2003
- Worm double whammy still hitting hard
  August 21, 2003
- VeriSign tracks buyers to fight e-fraud
  June 18, 2003
- **Get this story's "Big Picture"**

Related quotes

Quotes delayed 20+ minutes

▼ VeriSign Inc **VRSN** 17.33 -0.57 (-3.18%)

- BT lures consumers with free Wi-Fi
- Napster fills in the blanks with CD d
- Motorola banks on new gadgets, fea
- Study: Wi-Fi weaving its way into ho
- Microsoft expands Windows Server
- Sybase ships Panther-ready databa
- Spam keeps coming, but its senders
- Infineon adds a little flash
- Ximian software gets SuSE support
- Veritas bulks up its utility computing
- Real offers new tech, song store
- Year in review: Chipping away
- Intel fund to bolster consumer electr

Most popular headlin

- Gadgets have Macworld spotlight
- Apple unveils smaller iPod, new sof
- Microsoft readies new Mac Office
- Open-source databases gaining fav
- Microsoft abandons Smart Display e
- Computing giants to debut new gea
- Year in review: News.com special re
- Happy New Worm
- The duel of the dual-layer DVD form
- Writing an end to the bio of BIOS

Exhibit 6

News.com special report

WHY HACKERS ESCAPE

Organized, well-financed criminals stay a step ahead of the law

By Greg Sandoval
Staff Writer, CNET News.com
May 14, 2002, 4:00 a.m. PT

The nightmare for Ecount, an online gift certificate service, began last year when a hacker broke in to the company's system and stole personal information belonging to its customers.

HACKERS SWAP CREDIT CARD TIPS
Click here >

Nine months later, the criminal is still at large. The thief has brazenly taunted executives with repeated e-mails while staying ahead of investigators, deftly wiping away his electronic fingerprints and covering his tracks at every turn.

"We're sick to death of hearing from him," Ecount Chief Executive Matt Gillin said of the intruder, who has offered to return the information for a fee.

Although law enforcement agencies are quick to trumpet their occasional victories against cybercriminals, they are rarely able to track down hackers sophisticated enough to pull off such complicated heists. Few hackers of this caliber are arrested, and fewer still spend time behind bars.

CLEAN GETAWAY

Sophisticated hackers erase their tracks, making it nearly impossible to hunt them down. Here's how one hacker might get away with a list of credit card numbers.

The resulting frustration for investigators, companies and consumer victims raises a question that has persisted for years: Why are hackers able to elude capture so easily? The answer, according to security analysts and fraud investigators, is that the Internet has bred an elite class of criminals who are organized, well funded and far more technologically sophisticated than

most law enforcement officials.

"It's a world-class business," said Richard Power, editorial director of the Computer Security Institute, a private research firm that tracks electronic crime. "Al-Qaida and serious narcotic terrorists are using credit card fraud to finance their groups."

Fraud cost e-tailers $700 million in lost merchandise last year, says Avivah Litan, a financial analyst for research firm Gartner. Some large Internet retailers have software that screens transactions and refuses to sell to customers who appear suspicious. Litan estimates that this costs Web stores between 5 percent and 8 percent of sales.

A Gartner study also shows that 5.2 percent of online shoppers have been victimized by credit card fraud and 1.9 percent by identity theft.

"These are huge numbers. This is scary stuff," Litan said. "The Internet has got an albatross around its neck."

Special report
Cracking the nest egg ▶
Hackers find fortunes in online banking accounts

Skilled hackers shake off investigators by shuttling between multiple servers before launching an attack. After fleeing a targeted site with credit card numbers or other bounty, the intruders immediately begin deleting the log files of each server they have passed through, eliminating any record that they were there.

It is the equivalent of "vacuuming up the crime scene," said independent fraud investigator Dan Clements, who runs a Web site devoted to catching hackers called CardCops.com. Only about 10 percent of active hackers are savvy enough to work this way consistently, he said, but they are almost always successful.

Having grown up with the breakneck pace of "Internet time," hackers of this digital generation use speed as a primary weapon. As with all criminal investigations, pursuing online suspects means time-consuming records searches that often require subpoenas–a process that can give hackers an insurmountable advantage.

FBI agents can swiftly get subpoenas from the courts but often lose critical time trying to serve them. Agents can spend days sorting through digital smoke screens created by multiple servers, requiring agents to obtain and serve multiple subpoenas.

"AL-QAIDA AND SERIOUS NARCOTIC TERRORISTS ARE USING CREDIT CARD FRAUD TO FINANCE THEIR GROUPS."
-Richard Power, editorial director, Computer Security Institute

In the meantime, valuable evidence is often lost, and by then, hackers are long gone.

The federal government is taking steps to improve its fight against criminal activity online. FBI Director Robert S. Mueller created a new cybercrime unit in December, and the Bush administration has added 50 new federal prosecutors to address the problem nationwide.

Still, few believe that these measures will eradicate a problem that's become so deeply entrenched. The FBI confirmed, for example, that no arrests have been made in any of six recent high-profile cases reviewed by CNET News.com:

• **Playboy.com**: An intruder slipped past the Web site security systems of the adult entertainment company last November and obtained the personal information of an undisclosed number of customers of the site's e-commerce store. The hacker notified customers that he or she had pilfered the information and, as proof, gave them their credit

Cloaked code corporate secu
Hackers find n bilk eBay user
Pacific Rim a for hack attack
Tools for a mo Internet
Deciphering th myth
Playboy says stole custome
Hacker disclos after demands
As Net fraud g do e-tailers' fe
Hack at Amaz service expos thousands
Online stores the doors
FBI looking int questionable c charges
Company say try exposes th of card numbe
Hacker attack string of online card thefts
AmEx, Discov to replace card security breac
FBI probes ex case at CD sto

News arou the Web
U.S. hacker se

card numbers.

• **Ecount**: Last summer, a hacker circumvented the Internet defenses of the Philadelphia-based company's gift certificate service and notified customers of the breach in an e-mail that included their home addresses. The hacker then demanded $45,000 from the company to keep him from exposing the personal information of 350,000 customers.

• **Egghead.com**: A hacker infiltrated the e-tailer's system in December 2000. After three weeks of investigation, the company said the intruder did not obtain the personal information of its 3.7 million customers, but many banks said they spent millions of dollars to issue new credit cards in the meantime.

• **Creditcards.com**: Also in December 2000, a hacker broke in to systems maintained by the company, which enables merchants to accept payments online, and made off with about 55,000 credit card numbers. The hacker tried to extort the company and, when executives refused to pay, exposed the numbers by posting them on the Web.

• **Western Union**: In September 2000, a hacker exploited an opening in the Web site of the financial services company and got away with more than 15,000 credit card numbers. Human error left "performance management files" open on the site during routine maintenance, allowing the hacker access.

• **CD Universe**: About 350,000 credit card numbers were stolen from the online music company in January 2000, one of the first large-scale hackings of its kind. The thief, identified only as "Maxus," held the card numbers hostage and demanded a $100,000 ransom. When the company refused, the hacker posted the numbers on a Web site.

Without commenting on these specific cases, law enforcement officials say many online merchants may be partly to blame for the lack of arrests because they do not devote enough resources to prevent intrusion or facilitate investigations in the event of a crime.

"If there is any message to get out there, it would be for companies to upkeep their antivirus and firewall software," said Laura Bosley, a spokeswoman for the FBI's Los Angeles field headquarters.

UNSOLVED HACKS

The people who stole credit card numbers from these major online merchants are still at large.

Company	Date	What they stole; additional crimes
Playboy.com	Nov 2001	Undisclosed number of credit card numbers; extortion
Ecount	Aug 2001	Personal customer information; extortion
Western Union	Sep 2000	15,000 card numbers
Creditcards.com	Dec 2000	55,000 card numbers exposed on the Web; extortion
Egghead.com	Dec 2000	3.7 million credit cards threatened*
CD Universe	Jan 2000	350,000 card numbers posted online; extortion

* Egghead announced that a hacker had accessed its computer system, "potentially including (its) customer databases."

Source: CNET News.com research

Jennifer Granick, litigation director at the Stanford Law School Center for Internet and Society, said security is often neglected by companies more interested in making a quick buck.

E-commerce companies "rushed online during the dot-com boom, and they saw the money that was to be had and didn't give a thought to security," she said. "They were too busy trying to capture eyeballs to secure their sites."

Even if they have fortified their Web sites against attack, many companies are still unaware of the importance of preserving evidence if a crime occurs--ignorance that can kill any hope of catching a perpetrator, said Bruce Smith, an investigator for Pinkerton Consulting & Investigations and a former FBI agent who worked on computer crime cases

in worldwide c
The Washington

White-collar crimefighters
Business 2.0

Experience is security start-u
Washtech.com

Lab will help F high-tech case
The Kansas City St

The saint of e-commerce? N
FBI's "Gotcha" pag

Russian comp hacker convic
U.S. Department o

Editors: Mike Yam Wilson, Lara Wrigh Balderama
Design: Ellen Ng
Production: Ben H

for six years.

Frequently, Smith said, agents will scan the Web logs of a hacked company only to find a blank record that leaves the intruder's trail stone cold. Sometimes, he said, the shopkeeper accidentally destroys the logs, covering the hacker's tracks with other records. More often, the online store never turns on the logging feature to begin with because it could slow a Web site's performance.

News.com video

"You cross your fingers when you start looking at the logs," Smith said. "Sometimes you get lucky, sometimes not."

Hackers expose credit card numbers
Chris Rouland, Internet Security Systems
December 13, 2000

Moreover, precious time can be lost when companies hesitate to contact authorities immediately after an intrusion. The reason for the delay is often rooted in business, not justice.

"Fear," Smith said. "They're reluctant to admit that they've been victimized. You can imagine the bad press. Here's someone who's telling clients their information is safe at the same time their site is getting hacked."

Security experts blasted Egghead for taking weeks to investigate whether the personal information of its customers had been compromised. A company with good logging capability should have been able to determine the extent of the intrusion within a few days, security specialists said, perhaps saving banks a cost of between $5 and $25 for each new credit card issued out of precaution.

"I think there was some things that we wished we did before the attack," said Jeff Sheahan, the former chief executive of Egghead. "We thought we had a tight oversight system. We asked ourselves how we missed this. It was just focusing on other things and not sensing that there was a big enough risk."

The investigation was expensive for Egghead, but the intrusion exacted a much higher price in the form of lost confidence among its customers. "When you're an e-commerce business, trust is important. I don't think there is any doubt that trust level took a hit to some degree," Sheahan said.

E-COMMERCE COMPANIES ARE "RELUCTANT TO ADMIT THAT THEY'VE BEEN VICTIMIZED. YOU CAN IMAGINE THE BAD PRESS."

-Bruce Smith, investigator, Pinkerton Consulting & Investigations

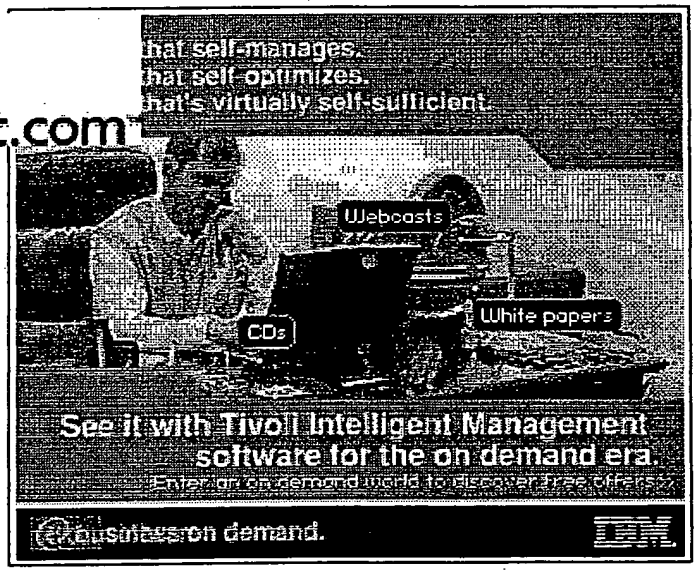
Other online merchants would do well to learn from Egghead's mistakes, for the number of hackings is growing. To gauge this trend, CardCops' Clements posted fake credit card numbers on the Web and then spread the word at sites popular with "carders"--those who traffic in stolen credit cards--that a Web site had accidentally divulged the information.

In less than a half-hour, the site had 74 visitors from 31 countries. Within a couple of days, the number of visitors had grown to 1,600. No one can say how many came to the site with criminal intent, but Clements believes most did.

"There's a war raging online," he said, "and the bottom line is that law enforcement is losing."

Exhibit 7

dc.internet.com



August 22, 2003 Hackers Tap Navy Credit Card System

By dc.internet.com Staff

Special Reports

A Department of Defense (DOD) investigative team is researching the recent hack of a

Will Office 2003 Change Everything?

Microsoft is preparing users for the launch of Office 2003, as it supplies the front-end interface to turn everyone into XML authorers, whether they realize it or not. The company says information will become reusable and flexible to a degree never before experienced.

Navy system that gained access to 13,000 purchase cards issued by Citibank. The Navy has subsequently cancelled all of its approximately 22,000 purchase cards.

According to a statement issued by the DOD Purchase card Management Program, "Vendors who accept the purchase card and do business with the Navy should be aware that all card accounts have been cancelled and that Citibank is working quickly to re-establish new accounts and cards. In the meantime, emergency purchases are being handled on a case-by-case basis to fully support Navy requirements,."

The hack was another in a string of security problems the Navy has had with its credit cards. Last year, a General Accounting Office (GAO) investigation revealed widespread abuse in the program including unauthorized purchases that included plastic surgery and home computers. Cardholders have defaulted on several million dollars worth of purchases.

[more]

Hot Topics
•Frauds, Scams and the Flimflam-Man
•Advertising's Hottest Sector - Paid Search
•The Blackout of 2003
•DMCA Subpoenas: Supreme Battle Brewing?
•SCO Declares War on Linux

Stats
•E-mail Around The World, July 2003
•Cable TV Suffers From Higher Rate Increases, Lower Satisfaction
•Prospects Brighten for Worldwide PC Sales
•The ASPnews Top 50 -- August Update
•Etailers Are Hard on Themselves

DC News

NY News

SiliconValley News

email

select a newsletter above, type your email and click the arrow to sign up!

Navy officials declined to comment on what system was breached in the hack, but promised to take appropriate measures to secure its systems. At the time of the GAO report, the DOD said it was using data mining techniques to track fraud.

Email this article Print this article

internet.com

Internet News
Internet Investing
IT
Windows Technology
Linux/Open Source
Developer
Interactive Marketing
xSP Resources
Small Business
Wireless Internet
Downloads

News Archives

Current Headlines by topic

Advertising
•Switchboard Rolls Out Paid Link Program
•Sobig.F Weekend Attack Thwarted; Feds Hunt Source
•Ask Jeeves Adds Search Tools

Business
•Thomson Aims to Beef Up Scientific Arm
•McData Nabs Two Storage Networking Businesses
•Hackers Tap Navy Credit Card System

Developer
•Q&A: JBoss CEO Marc Fleury
•MontaVista Says SCO Not A Threat to Embedded Linux

Enterprise
•Utility Computing Shines in Blackout
•Q&A: JBoss CEO Marc Fleury
•IBM's Rational to Update Progress at Conference

Finance
•Intel Chips Start Flying Off the Shelves
•Corel Shareholders Vote in Favor of Vector Buyout
•HP's Profits Improve But Disappoint

Infrastructure
•McData Nabs Two Storage Networking Businesses
•New Phase of Sobig.F Set for Fridays
•Intel Chips Start Flying Off the

Storage
•McData Nabs Two Storage Networking Businesses
•Sun, Hitachi Refresh Storage Ties
•Gateway Eyes Dell's Server Model for Storage

Wireless
•Gallagher Nominated for NTIA's Top Spot
•Court Overturns Palm/3Com Patent Case
•Despite Losses, Hutchison Sticks with 3G Strategy

xSP
•Macromedia Retools MX Line
•Level 3, SBC Extend Dial-Up

Internet Resources
Internet Lists
International EarthWeb
Career Resources

Search internet.com
Advertise
Corporate Info
Newsletters
E-mail Offers

•IBM's Rational to Shelves Update Progress at Conference

Ecommerce

•E-Commerce On a Steady Rise
•Contextual Ad Debate Rouses Critics
•priceline.com Expands Travel Service

Stats

•E-mail Around The World, July 2003
•Cable TV Suffers From Higher Rate Increases, Lower Satisfaction
•Prospects Brighten for Worldwide PC Sales

Deal
•Utility Computing Shines in Blackout

Regional News

•3Com, Aspect Target Enterprises, Call Centers
•GAO: Archives' Proposed System Lacks Key Elements

Contact internetnews.com staff

Exhibit 8

FTC FACTS for Consumers

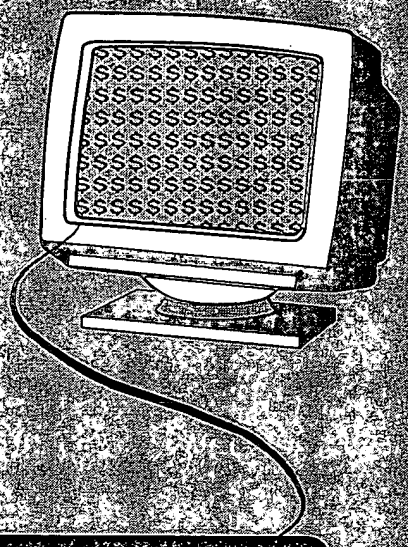
FOR THE CONSUMER

FEDERAL TRADE COMMISSION

1-877-FTC-HELP

www.ftc.gov

A Consumer's Guide to e-Payments



credit

Charge

debit

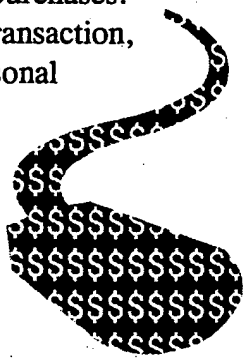
stored-value

The Internet has taken its place beside the telephone and television as an important part of people's lives. Consumers use the Internet to shop, bank and invest online. Most consumers use credit or debit cards to pay for online purchases, but other payment methods, like "e-wallets," are becoming more common.

The Federal Trade Commission (FTC) wants you to know about these payment technologies and how to make your transactions as safe and secure as possible. Keep these tips in mind as other forms of electronic commerce, like mobile and wireless transactions, become more available.

AND HOW WOULD YOU LIKE TO PAY?

Most online shoppers use credit cards to pay for their online purchases. But debit cards — which authorize merchants to debit your bank account electronically — are increasing in use. Your debit card may be an automated teller machine (ATM) card that can be used for retail purchases. To complete a debit card transaction, you may have to use a personal identification number (PIN), some form of a signature or other identification, or a combination of these identifiers. Some cards have both credit and debit features: You select the payment



option at the point-of-sale. But remember, although a debit card may look like a credit card, the money for debit purchases is transferred almost immediately from your bank account to the merchant's account. In addition, your liability limits for a lost or stolen debit card and unauthorized use are different from your liability if your credit card is lost, stolen or used without your authorization.

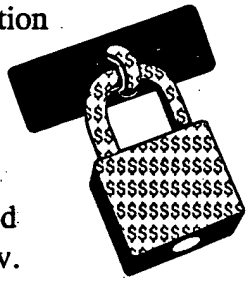
Other electronic payment systems — sometimes referred to as "electronic money" or "e-money" — also are now common. Their goal is to make purchasing simpler. For example, "stored-value" cards let you transfer cash value to a card. They're commonly used on public transportation, at colleges and universities, at gas stations, and for prepaid telephone use. Many retailers also sell stored-value cards in place of gift certificates. Some stored-value cards work offline, say, to buy a candy bar at a vending machine; others work online, for example, to buy an item from a website; some have both offline and online features. Some cards can be "reloaded" with additional value, at a cash machine; other cards are "disposable" — you throw them away after you use all their value. Some stored-value cards contain computer chips that make them "smart" cards: These cards may act like a credit card

as well as a debit card, and also may contain stored value.

Some Internet-based payment systems allow value to be transmitted through computers, sometimes called "e-wallets." You can use "e-wallets" to make "micropayments" — very small online or offline payments for things like a magazine or fast food. When you buy something using your e-wallet, the balance on your online account decreases by that amount. "E-wallets" may work by using some form of stored value or by automatically accessing an account you've set up through a computer system connected to your credit or debit card account.

"PAYING" IT SAFE

The FTC encourages you to take steps to make sure your transactions are secure and your personal information is protected. Although you can't control fraud or deception on the Internet, you can take action to recognize it, avoid it and report it. Here's how.



- **Use a secure browser** — software that encrypts or scrambles the purchase information you send over the Internet — to help guard the security of your information as it is transmitted to a website. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available

from the manufacturer. You also can download some browsers for free over the Internet. When submitting your purchase information, look for the "lock" icon on the browser's status bar, and the phrase "https" in the URL address for a website, to be sure your information is secure during transmission.

- **Check the site's privacy policy**, before you provide any personal financial information to a website. In particular, determine how the information will be used or shared with others. Also check the site's statements about the security provided for your information. Some websites' disclosures are easier to find than others — look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If you're not comfortable with the policy, consider doing business elsewhere.

- **Read and understand the refund and shipping policies** of a website you visit, before you make your purchase. Look closely at disclosures about the website's refund and shipping policies. Again, search through the website for these disclosures.

- **Keep your personal information private.** Don't disclose your personal information — your address, telephone number, Social Security number, bank account number or e-mail address — unless you know who's collecting the information, why they're collecting it and how they'll use it.
- **Give payment information only to businesses you know and trust,** and only when and where it is appropriate — like an order form. Never give your password to anyone online, even your Internet service provider. Do not download files sent to you by strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your modem.
- **Keep records of your online transactions and check your e-mail** for contacts by merchants with whom you're doing business. Merchants may send you important information about your purchases.
- **Review your monthly credit card and bank statements** for any errors or unauthorized purchases promptly and thoroughly. Notify your credit or debit card issuer immediately if your credit or debit card or checkbook is lost or stolen, or if you suspect someone is using your accounts without your permission.

REPORT PROBLEMS IMMEDIATELY

The Fair Credit Billing Act (FCBA) and Electronic Fund Transfer Act (EFTA) establish protections against lost or stolen credit or debit cards, and procedures for resolving errors on credit and bank account statements that can include:

- credit charges or electronic fund transfers that you — or anyone you've authorized to use your account — have not made;
- credit charges or electronic fund transfers that are incorrectly identified or show the wrong amount or date;
- computation or similar errors;
- a failure to properly reflect payments or credits, or electronic fund transfers;
- not mailing or delivering credit billing statements to your current address, as long as that address was received by the creditor in writing at least 20 days before the billing period ended; and
- credit charges or electronic fund transfers for which you request an explanation or documentation, because of a possible error.

For credit: The FCBA generally applies to "open end" credit accounts — that is, credit cards and revolving charge accounts, like department store accounts. It does not apply to loans or credit sales that are paid according to a fixed schedule until the entire amount is paid back, like an automobile loan.

Lost or stolen credit cards: Under the FCBA, your liability for lost or stolen credit cards is limited to $50. If the loss involves only your credit card number (not the card itself), you have no liability for unauthorized use. It's best to notify your card issuer promptly upon discovering the loss. Many companies have toll-free numbers and 24-hour service to deal with such emergencies. Always follow up with a letter and keep a copy for your records.

Billing errors: The FCBA's settlement procedures apply to disputes about "billing errors" for open-end accounts, including unauthorized charges (you cannot be liable for more than $50 for unauthorized credit charges); charges for goods or services you didn't accept or weren't delivered as agreed; charges that are incorrectly identified or show the wrong amount or date; math errors; a failure to properly reflect payments or credits; not mailing or delivering credit billing statements to your current address, if the address was received by the creditor in writing at least 20 days before the billing period ended; and charges for which you request an explanation or documentation, because of a possible error.

For more information on e-commerce and the Internet, visit www.ftc.gov.

To take advantage of the FCBA's consumer protections for errors on your account, write to the creditor at the address given for "billing inquiries," not the address for sending your payments. Include your name, address, account number and a description of the billing error. Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. And if you send your letter by certified mail, return receipt requested, you'll have proof that the creditor received it. Include copies (not originals) of sales slips or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your dispute in writing within 30 days after it is received, unless the problem is resolved within that period. The creditor must conduct an investigation and either correct the mistake or explain why the bill is believed to be correct, within two billing cycles (but not more than 90 days), unless the creditor provides a permanent credit instead. You may withhold payment of the amount in dispute and any related finance charges and the creditor may not take any action to collect that amount during the dispute.

For debit: The EFTA applies to electronic fund transfers — transactions involving automated teller machines (ATMs), debit cards and other point-of-sale debit transactions, and other electronic banking transactions that can result in the withdrawal of cash from your bank account.

Lost or stolen debit cards: If someone uses your debit card, or makes other electronic fund transfers, without your permission, you can lose from $50 to $500 or more, depending on when you report the loss or theft. If you report the loss within two business days after you discover the problem, you will not be responsible for more than $50 for unauthorized use. However, if you do not report the loss within two business days after you realize the card is missing, but you do report its loss within 60 days after your statement is mailed to you, you could lose as much as $500 because of an unauthorized withdrawal. And, if you do not report an unauthorized transfer or withdrawal within 60 days after your statement is mailed to you, you risk unlimited loss. That means you could lose all the money in your account and the unused portion of your maximum line of credit established for overdrafts.

Some financial institutions may voluntarily cap your liability at $50 for certain types of transactions, regardless of when you report the loss or theft; because this is voluntary, their policies could change at any time. Ask your financial institution about its liability limits.

EFT errors: The EFTA's error procedures apply to certain problems. This can include:

- electronic fund transfers that you — or anyone you've authorized to use your account — have not made;

- incorrect electronic fund transfers;
- omitted electronic fund transfers;
- a failure to properly reflect electronic fund transfers; and
- electronic fund transfers for which you request an explanation or documentation, because of a possible error.

To take advantage of the EFTA's error resolution procedures, you must notify your financial institution of the problem not later than 60 days after the statement containing the problem or error was sent. Although most financial institutions have a toll-free number to report the problem, you should follow-up in writing. For retail purchases, your financial institution has up to 10 business days to investigate after receiving your notice of the error. The financial institution must tell you the results of its investigation within three business days of completing its investigation. The error must be corrected within one business day after determining the error has occurred. If the institution needs more time, it may take up to 90 days, in many situations, to complete the investigation — but only if it returns the money in dispute to your account within 10 business days after receiving notice of the error, while it reviews your concerns.

For stored-value: The FCBA and the EFTA may not cover stored-value cards or transactions involving them, so you may not be covered for loss or misuse of the card. However, stored-value cards still might be useful for micropayments and

other small purchases online because they can be convenient and — in some cases — offer anonymity. Before you buy a stored-value card or other form of e-money, ask the issuer for written information about the product's features. Find out the card's dollar limit, whether it is reloadable or disposable, if there's an expiration date, and any fees to use, reload or redeem (return it for a refund) the product. At the same time, ask about your rights and responsibilities. For example, does the issuer offer any protection in the case of a lost, stolen, misused, or malfunctioning card, and who do you call if you have a question or problem with the card?

FOR MORE INFORMATION

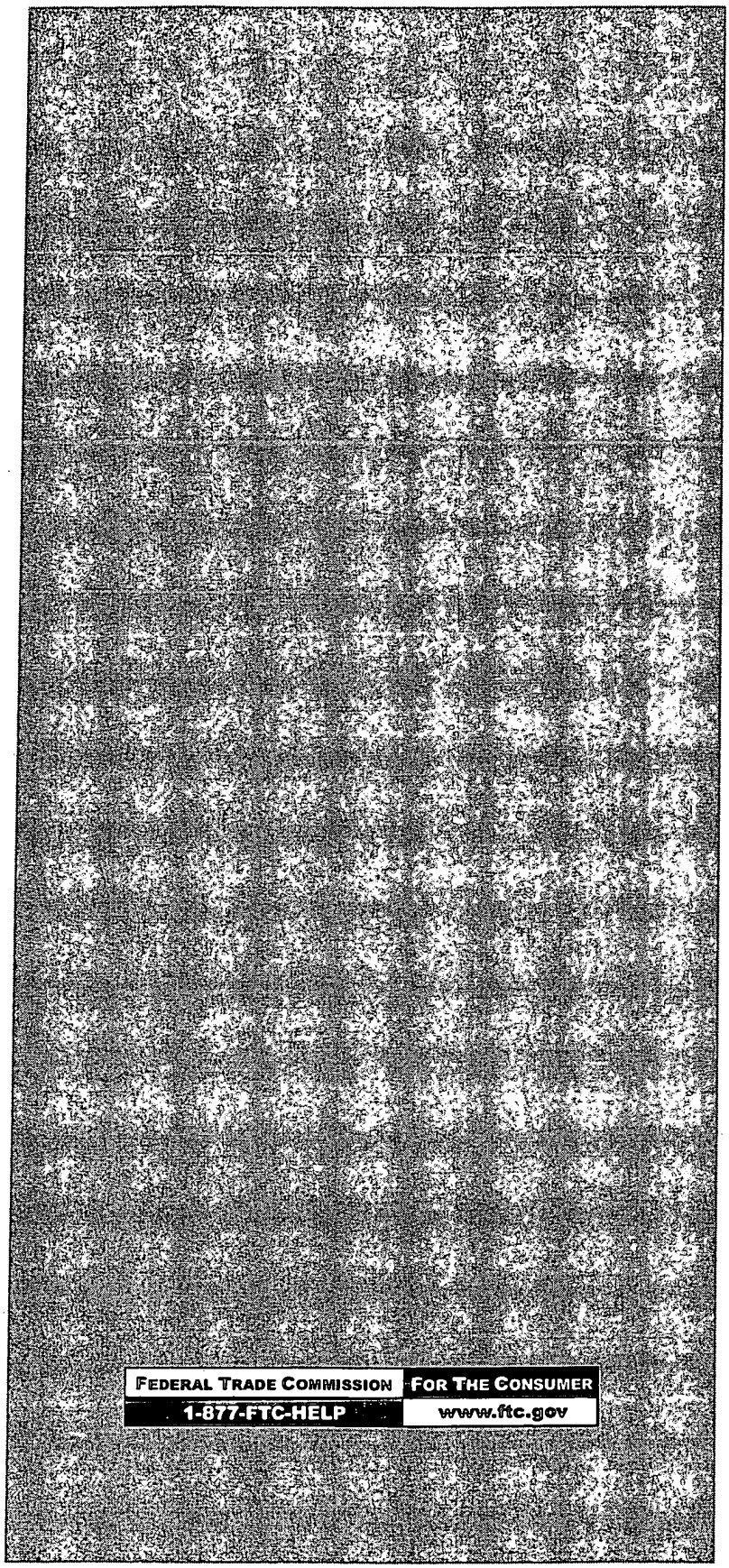
Your financial institution, local consumer protection agency and law enforcement agencies like the Federal Trade Commission or your state Attorney General are among the many organizations working to help consumers understand electronic commerce and new online payment options.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft

and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education

March 2003


FEDERAL TRADE COMMISSION
FOR THE CONSUMER
1-877-FTC-HELP
www.ftc.gov

Are you a victim? Click here.

Identity Theft Information Center™

FTC ID Theft Survey
Summary for Consumers

The third major national survey to appear in recent weeks confirms that identity theft is raging out of control and causing devastating economic damage.

September 2003

On September 3, 2003, the Federal Trade Commission released the results of a survey[1] conducted to clarify certain aspects of the crime of identity theft in the United States. The results were even more disturbing than the FTC had feared.

- 10 million Americans — 4.6% of the adult population — became victims of identity theft in the past year alone.
- 27 million Americans have been victimized within the past five years.
- Identity theft cost the U.S. economy nearly $53 billion last year.
- The incidence of identity theft increased by nearly 41% last year.

The original report (nearly 100 pages long) can be found on the FTC website. In this document, for your convenience, we've summarized the FTC survey's key findings for consumers in an accessible Q&A format.

- Do victims report their problem to local police? will a police report result?
- Are victims satisfied with police handling of their cases?

How serious is the crime of identity theft in the United States?

Very serious indeed — so serious, in fact, that researchers were shocked by what their survey revealed. In the past year, nearly **10 million Americans** — equivalent to 4.6 percent of the entire adult population — discovered that they had been victims of identity theft. 27 million Americans have been victimized in the past five years. What's more, last year the incidence of identity theft increased by nearly 41 percent over the year before — and it shows every sign of picking up speed.

Type of ID Theft Crime	Millions of People	Pct of Adult Population
New Account & Other Frauds	3.23	1.5%
Existing Credit Cards	5.17	2.4%
Other Existing Accounts	1.51	0.7%
All Identity Theft	9.91	4.6%

What's the impact of identity theft on the U.S. economy? Back to Top

In a word, horrendous. The FTC study indicates a total loss last year of **$52.6 billion**, including costs borne by individual victims and losses sustained by businesses and financial institutions. This amounts to **0.5% of the U.S. Gross National Product** for 2002.

Type of ID Theft Crime	Cost in Billions of Dollars to Victim Segments		
	Victims	Businesses	Total
New Account & Other Frauds	$3.8	$32.9	$36.7
[illegible]	[illegible]	[illegible]	[illegible]
All Identity Theft	$5.0	$47.6	$52.6

What's the cost of identity theft to the individual victim? Back to Top

This is a tricky question. For one thing, many victims' most meaningful losses are measured not in dollars and

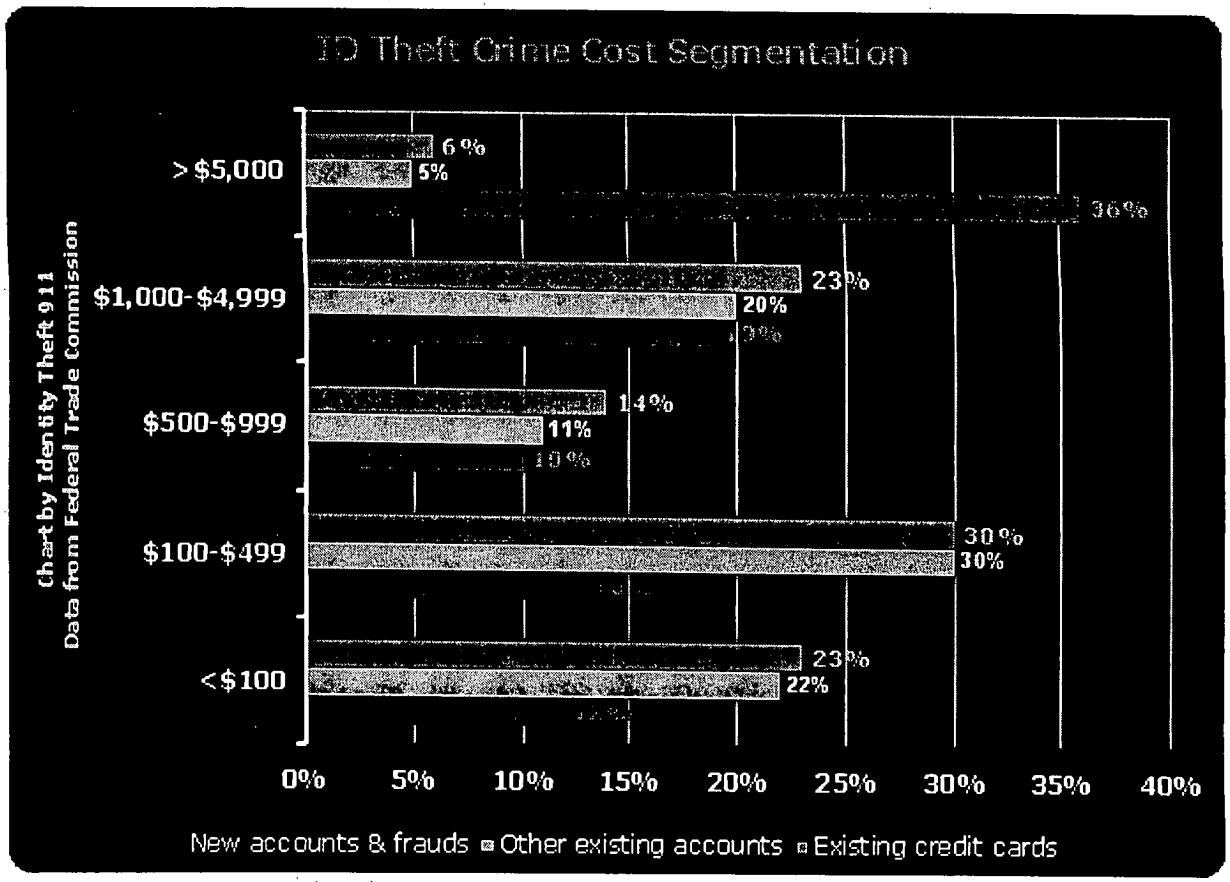
cents, but in wasted time, humiliation, stress, and damage to their financial security, reputation, and self-esteem.

From a strictly financial perspective, however, the FTC study found the average loss from the misuse of a victim's personal information to be about $4,800. For the most serious category of fraud related to identity theft — new accounts opened, new loans taken out, various other forms of fraud perpetrated — the ID thief's average haul was significantly higher: about $10,200 in money, goods, and services. From this we can derive a total loss to businesses, including financial institutions, of $33 billion from this type of identity theft over the last year alone.

While individuals whose information is misused bear a relatively small percentage of the overall cost of identity theft,[2] victims of all forms of identity theft still spent an average of about $500 dealing with their experience — which doesn't necessarily mean resolving it. Victims of the most serious category of fraud spent even more — an average of almost $1,200. The total annual cost of identity theft to individual victims is thus in the vicinity of $5 billion, with those in the most serious category bearing about $3.8 billion of that total.

Type of ID Theft Crime	Victim Hours Spent Resolving the Problem	Victim's Expenses Out-of-Pocket
New Account & Other Fraud	60	$1,180
All Identity Theft	30	$500

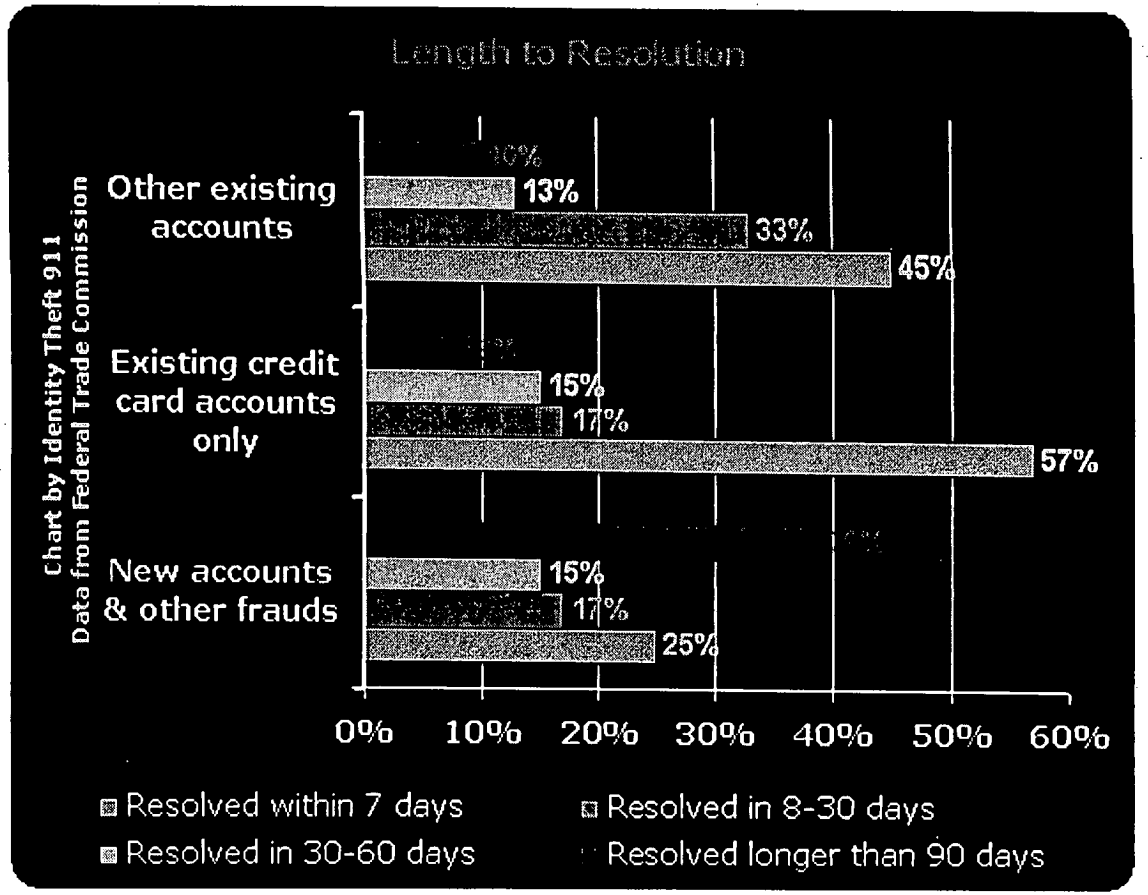
Victims of identity theft also spend a substantial amount of their own time resolving problems caused by criminal misuse of their personal information. On average, it comes to about 30 hours; for victims of the most serious category of fraud, it's double that. All told, Americans spent almost 300 million hours resolving problems related to identity theft in the past year, with almost two-thirds of that time (194 million hours) lost by victims in the most serious category.



How long does it take to resolve a case of identity theft completely? Back to Top

The time required to resolve a case of identity theft varies according to the severity of the crime, the victim's knowledge of the financial and law enforcement infrastructure, and the victim's persistence and skill in working with a broad range of businesses and governmental agencies. Adding to the victim's frustration, of course, is the very real possibility that if certain pieces of personal information have been compromised, the problem may never be fully resolved.

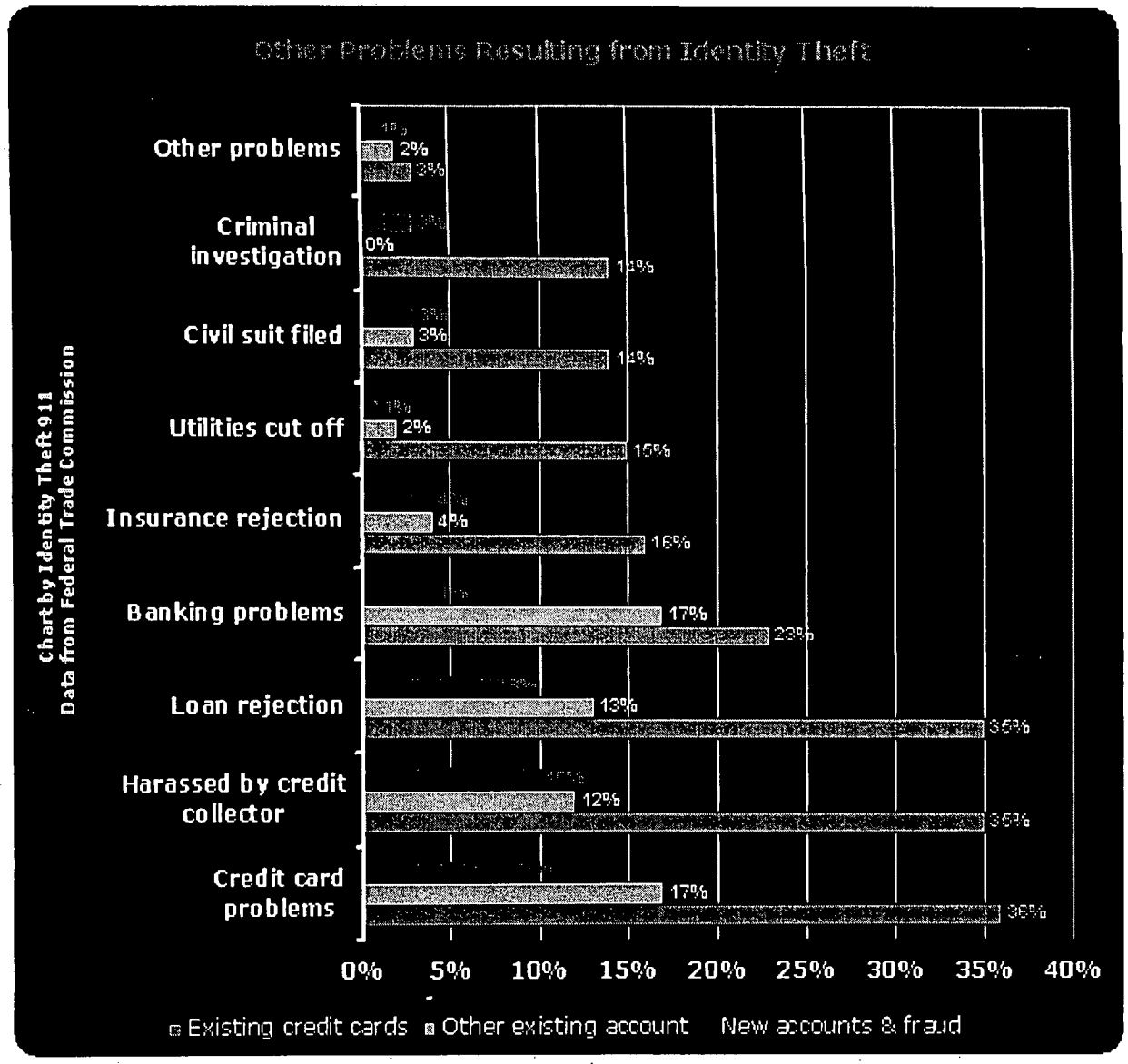
In general, the FTC study indicates that serious fraud problems stemming from identity theft require more than three months to resolve in 39 percent of the identified cases. Five percent of victims said the misuse of their identity was ongoing at the time of the survey; 21 percent indicated that they were still experiencing problems as a result of an earlier abuse.



Nevertheless, the study indicates that serious fraud problems require more than 3 months to resolve in 39% of the identified cases. Although 5% of the victims said the misuse of their identity was ongoing at the time of the survey, 21% indicated that they were still experiencing problems that were the result of an earlier misuse.

What other problems are associated with identity theft? Back to Top

A total of 36 percent of all victims of identity theft reported additional problems as a result of having their personal information misused. These additional complications can be quite severe. For instance, 20 percent of identity theft victims report being harassed by a debt collector; 18 percent report being turned down for a loan; and 13 percent report various banking problems.



Victims experiencing more serious forms of identity theft — those who have new accounts opened or new loans established in their name, or suffer other forms of fraud[3] using their personal identification — are far more susceptible to such problems, which can include criminal investigations and civil lawsuits. The likelihood of such problems increases with the amount of money involved. For example, cases involving more than $5,000 have a 74 percent probability of further complications. The likelihood of additional problems increases with complexity,

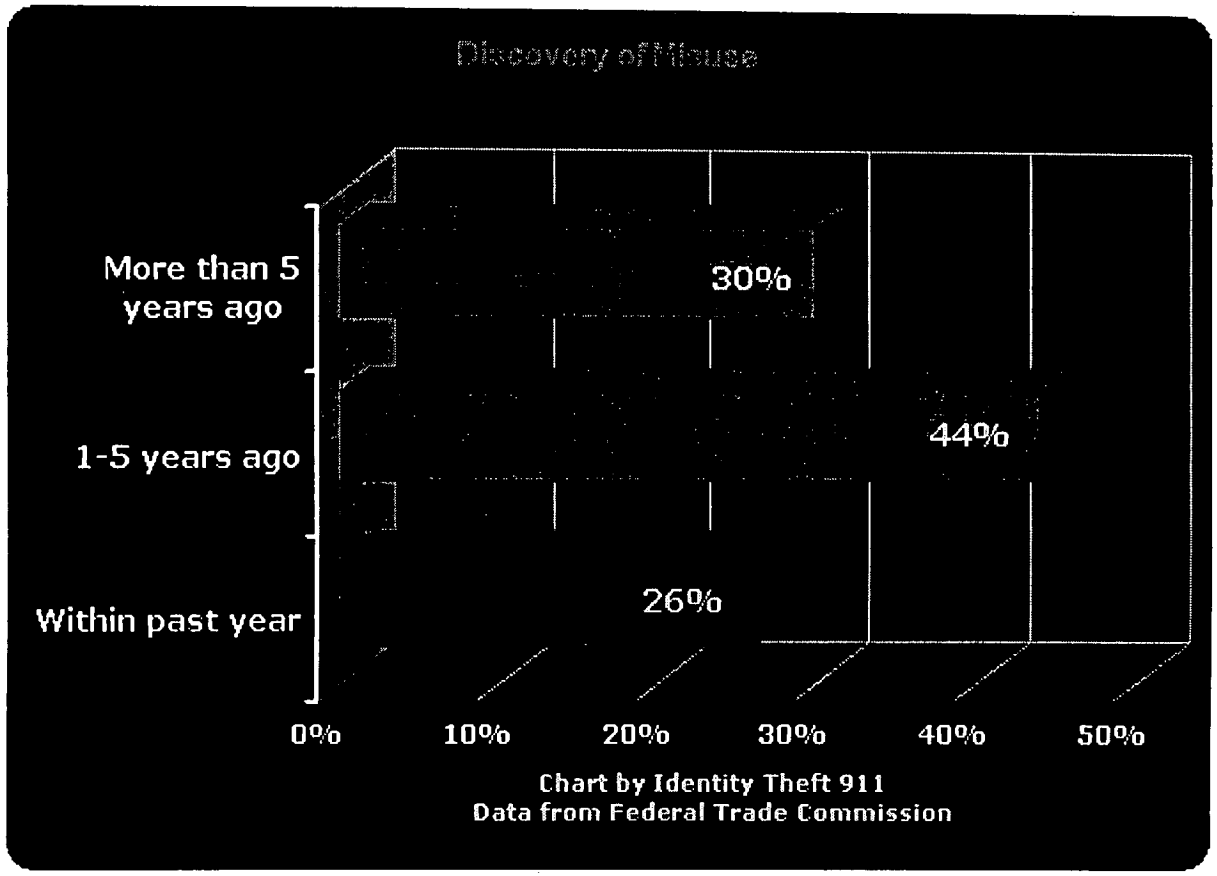
with 76 percent of victims who have suffered four or more distinct misuses of their identity being subjected to additional personal complications.

On the other hand, the faster the crime is detected, the less severe these complications tend to be. If it's discovered within one month, the probability drops to 26 percent; if it takes more than six months, it rises to 76 percent.

Is identity theft becoming more common?

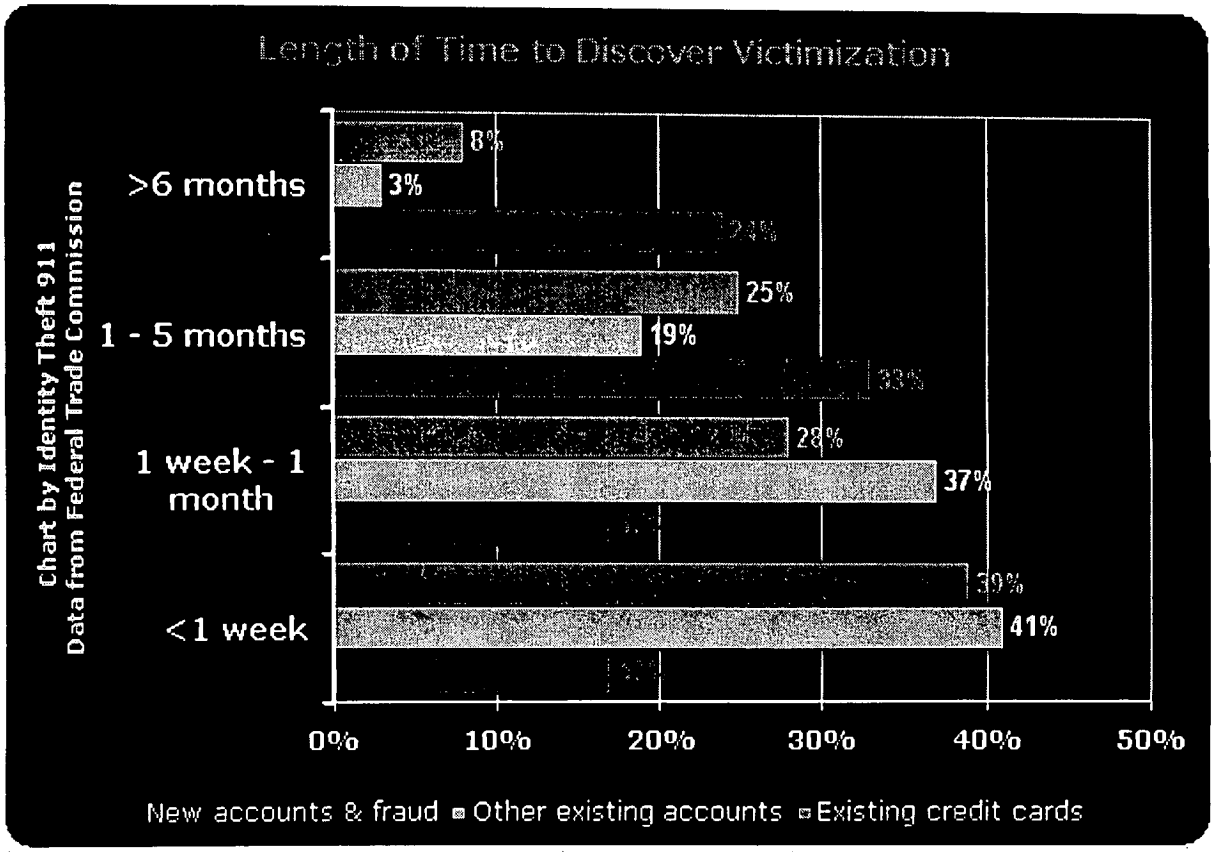
Back to Top

Without a doubt. The survey results show that incidents of identity theft are on the rise in the United States, and this increase has accelerated over the past two years. Overall, the number of victims of identity theft last year was **41 percent** higher than the previous year's tally.



How long does it take a victim of identity theft to discover the crime?

The most important determinant of this crime's severity — and, specifically, of the damage inflicted on the victim — is how long it takes for the identity theft to be discovered. While many victims recognized the problem within a week, those whose personal data was used to open new credit accounts, take out new loans, or engage in other types of fraud . precisely the ones whose financial exposure was greatest — were usually not so fortunate. In fact, 24 percent of this group took 6 months or more just to discover that the crime had taken place.



How long will the criminal abuse a victim's personal information? Back to Top

The median time period that victims' information was misused is between one week and one month. 12 percent of victims reported that their personal information was misused for 6 months; 25 percent said the abuse lasted no more than a day. Of those defrauded in more serious ways, more than 25 percent say the abuse continued

for over 6 months.

Who commits the crime of identity theft? Back to Top

In 26 percent of all cases, the victim knew who had misused their personal information. Of those who could identify the perpetrator, 35 percent said a family member or relative had misused their personal information; 18 percent named a friend, neighbor, or in-home employee; and 16 percent said the thief was a complete stranger whose identity they learned only after the fact. Six percent of victims said the responsible party worked at a company or financial institution with access to their personal information.

One interesting fact is that the more serious the abuse, the greater the likelihood that the victim knows the criminal's identity. Of those most seriously victimized (new accounts opened, new loans taken out, and so on), 34 percent were aware of the thief's identity, versus 18 percent of those for whom only existing accounts were abused.

In cases where the abuse involved only existing credit card accounts, someone at a financial institution or other company was cited as the source of the misused information by 33 percent of those who could identify the perpetrator. In cases involving new accounts and other fraud, 13 percent of those who knew the perpetrator's identity cited an employee of such a company, while 18 percent identified a family member or relative.

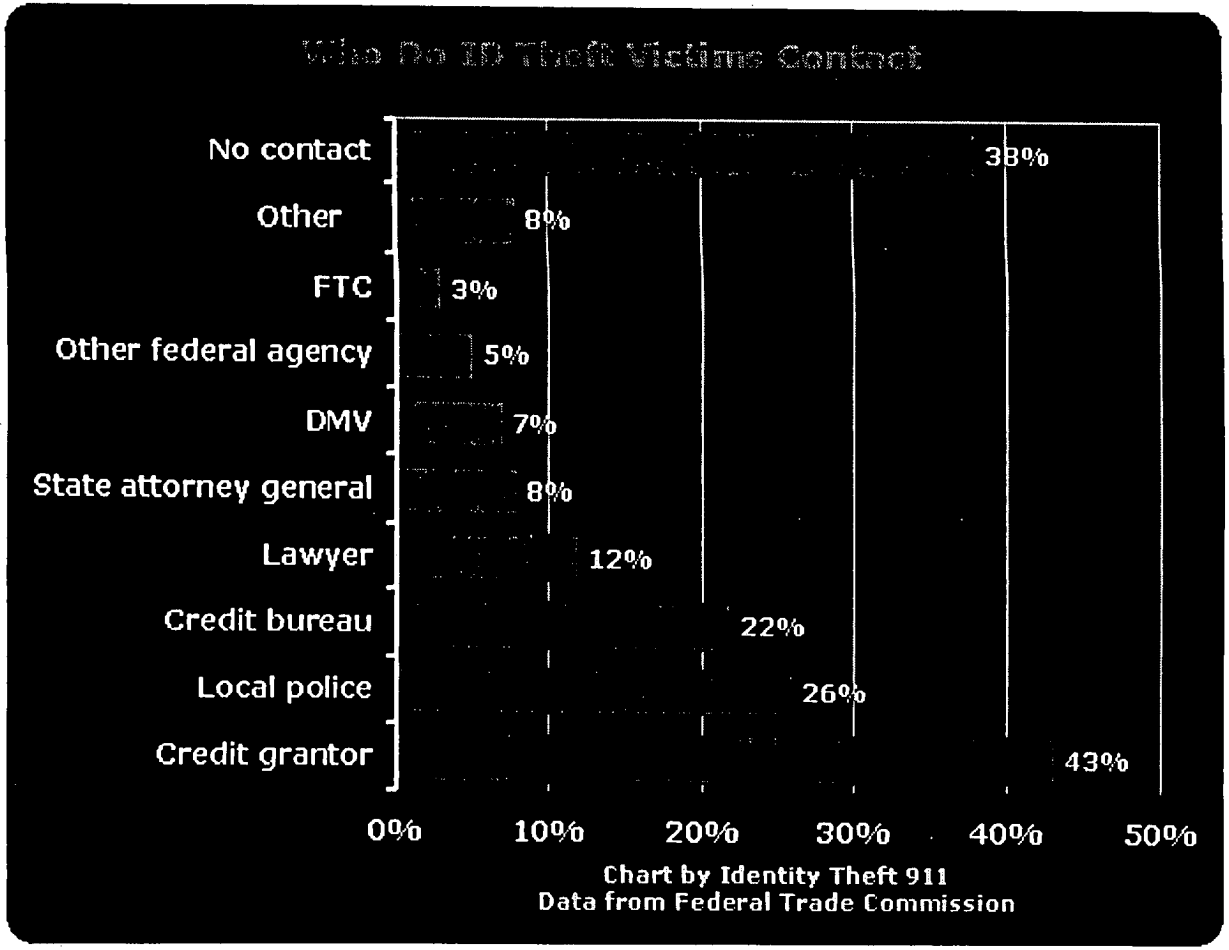
How do criminals steal personally identifying information? Back to Top

51 percent of victims say they know how identity thieves obtained their personal information. One-quarter of all victims say their information was lost or stolen. Fourteen percent cite a lost or stolen wallet, checkbook, or credit card; in the most serious category of abuse, however, only 8 percent attribute their loss to such a source. Four percent of all victims cited stolen mail as the source; of the most serious cases, 7 percent were attributed to mail theft.

Thirteen percent of all victims say their information was obtained in the course of a transaction, with personal information obtained from a credit card receipt or a purchase made by phone, by mail, or over the Internet.

Whom do victims of identity theft contact about their problem? Back to Top

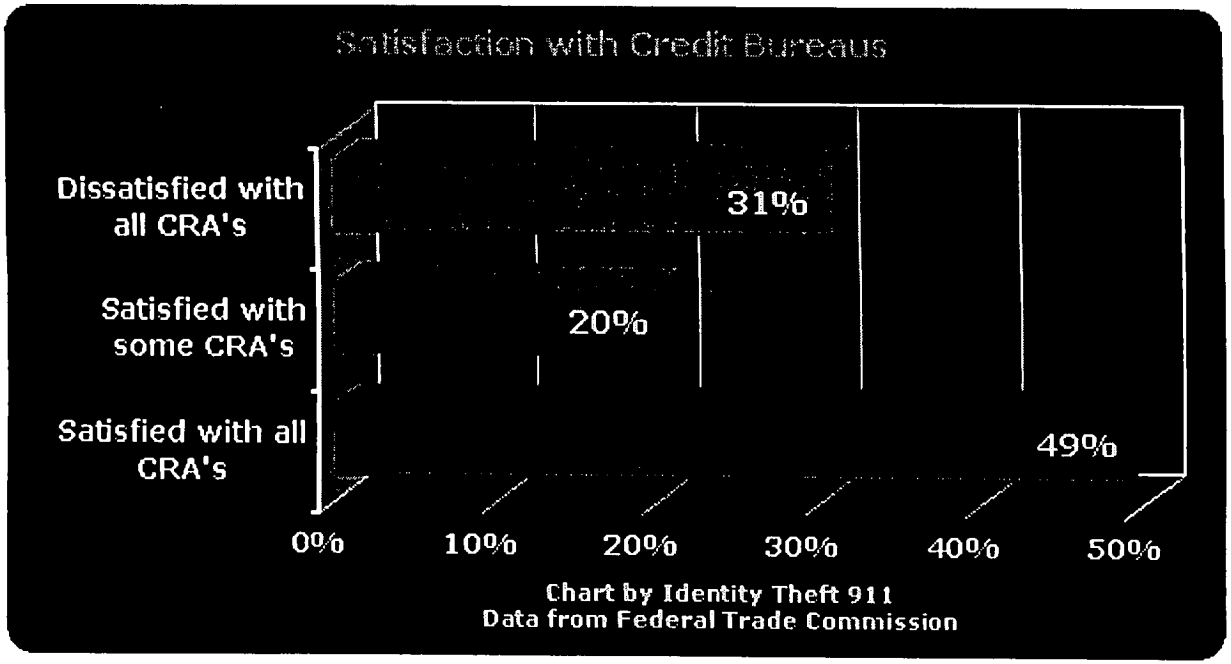
Victims of the more serious forms of identity theft were more likely to contact the police (17 percent) and the credit bureaus (37 percent). Somewhat surprisingly, only 13 percent of victims who had existing credit card accounts misused said they contacted a credit reporting agency. Five percent of victims contacted other federal agencies, including the U.S. Postal Service and the Social Security Administration.



Older victims were less likely to report having been victimized. Of victims aged 18-24, 83 percent reported their experience, whereas only 34 percent of victims 65 and older reported the crime.

Are victims of identity theft satisfied with the credit bureaus' performance? Back to Top

Of those victims who contacted more than one credit reporting agency, nearly half were satisfied with all of the agencies they spoke to; 20 percent expressed satisfaction with some of the agencies contacted, but not with others; and 31 percent were dissatisfied with all of the agencies they contacted.

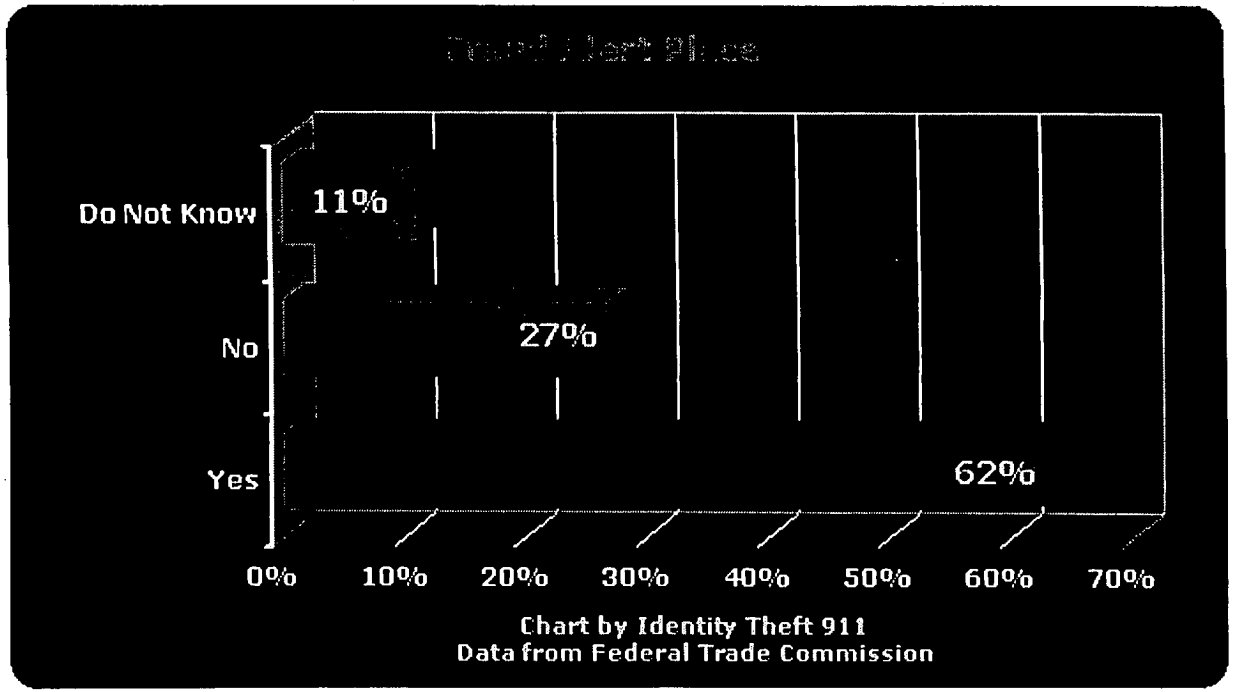


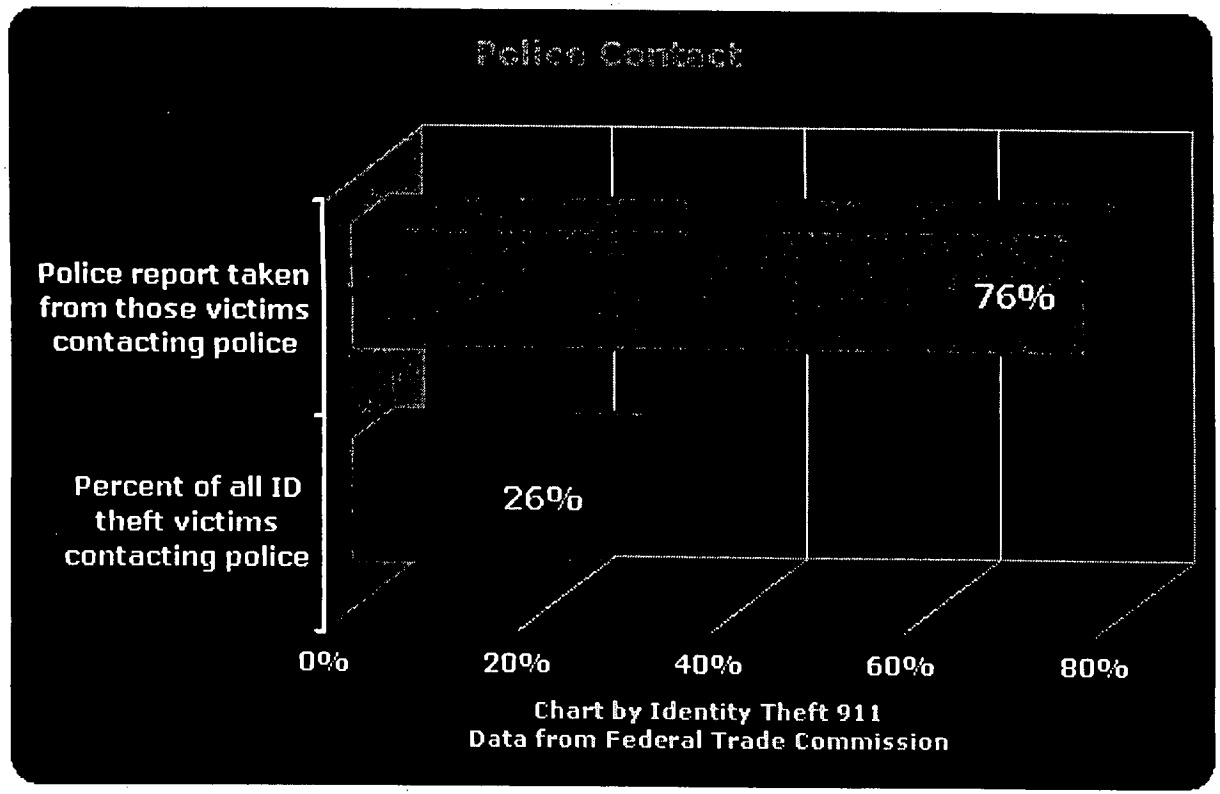
Do victims use the fraud alert option with credit reporting agencies? Back to Top

Less than one victim in four (22 percent) contacted at least one credit reporting agency; of those who did, 62 percent had fraud alerts added to their credit reports. Among those who did contact a credit bureau, 70 percent of those suffering the most serious forms of identity theft added a fraud alert to their files, versus 46 percent of those suffering only the misuse of an existing credit card account.

Do victims report their problem to local police? Will a police report result? Back to Top

Only 26 percent of identity theft victims surveyed reported the crime to local police. Of those cases, however, 76 percent resulted in a police report.

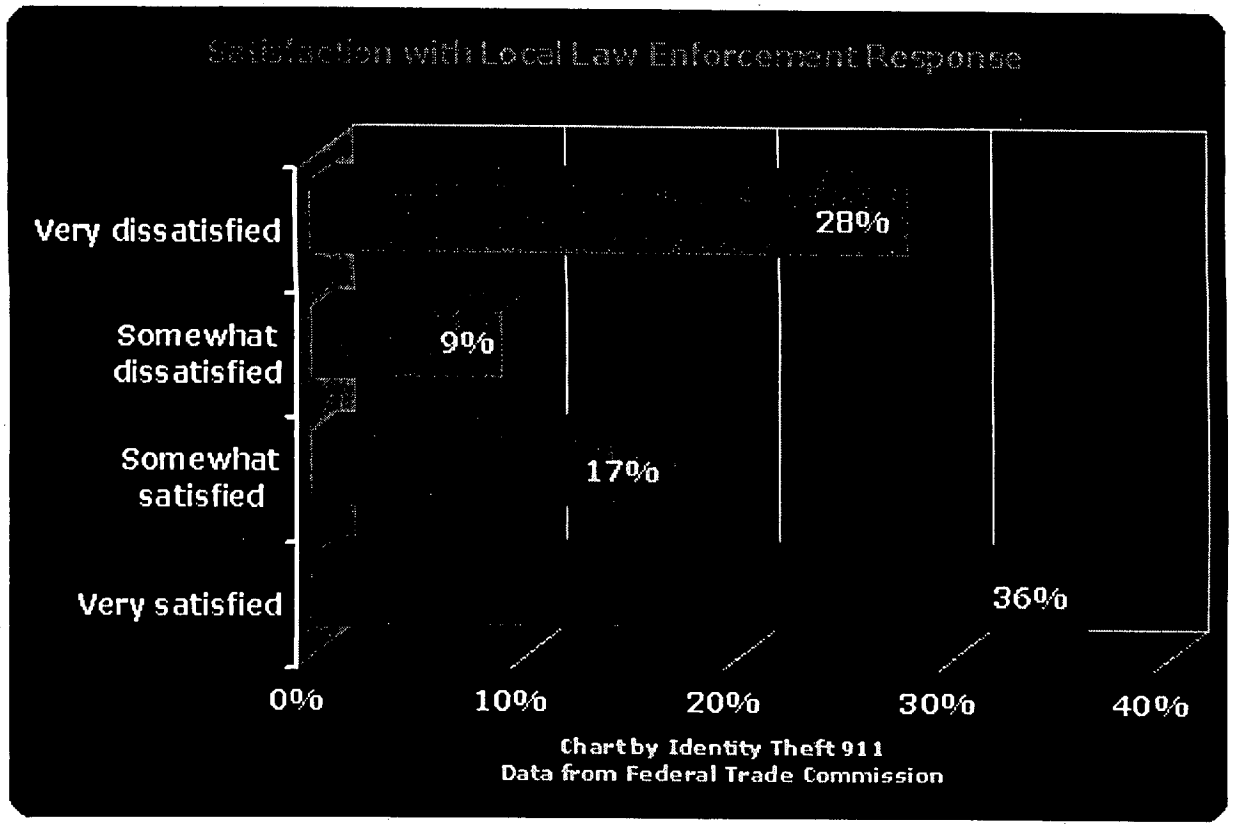

Do Not Know
No
Yes
11%
27%
62%
0%
10%
20%
30%
40%
50%
60%
70%
Chart by Identity Theft 911
Data from Federal Trade Commission



Are victims satisfied with police handling of their cases?

Back to Top

Some are satisfied, others thoroughly dissatisfied. One factor worth noting: Police were far more likely to take a report if the abuse was uncovered relatively quickly. Where the crime was discovered within five months, a report was taken 83 percent of the time. Where it took six months or more, the figure drops to 47 percent.



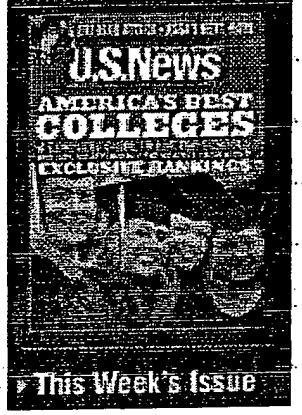
REFERENCES & NOTES:

[1] Federal Trade Commission . Identity Theft Survey Report. September 2003. Prepared by Synovate, 1650 Tyson Boulevard, Suite 110, McClean, Virginia 22102.

[2] Victims are generally not liable for losses based on fraudulent actions taken by identity thieves using their personal information. A variety of laws limit consumers' liability in these situations. Such laws include the Truth in Lending Act, 15 U.S.C. § 1601 et seq., implemented by Regulation Z, 12 C.F.R. § 226; see especially 15 U.S.C. § 1643; 12 C.F.R. § 226.12(b) (limits consumer liability for unauthorized credit card charges to a maximum of $50), and the Electronic Fund Transfer Act, 15 U.S.C. § 1693 et seq., implemented by Regulation E, 12 C.F.R. § 205; see especially 15 U.S.C. § 1693g; 12 C.F.R. § 205.6(b) (limits consumer liability for unauthorized electronic fund transfers depending upon the timing of consumer notice to the applicable financial institution). Consumer liability for losses associated with check fraud and loan fraud are typically limited by state statute or common law.

[3] "Other Frauds" include misuse of the victim's information to misrepresent a person's identity when someone is charged with a crime by law enforcement authorities, when renting an apartment or home, when obtaining medical care or employment with the victim's information, and similar misuses.

■



Rankings & Guides
Money & Business
Education
Health
Columnists
Technology
Best of the Web
Life Online
Gadgets
Privacy
Washington Whispers
Work & Career
News Briefings
Past Issues
News Quiz
Photography
U.S. News Store
Customer

High-tech card fraud goes on right behind your back

By Margaret Mannix

Do you know where your credit card is? Safely tucked inside your wallet, you say. But how safe is your account, never mind the card? These days, a credit card *number* is a valuable commodity to thieves. "You don't need the plastic to use somebody's credit card number," particularly in this era of Internet and catalog shopping, says Beth Givens, director of the Privacy Rights Clearinghouse in San Diego. The same applies to debit cards. A thief armed with a debit card number can go on a shopping spree, financed by your checking account.

Tech-savvy criminals are devising new ways to get their hands on card information. They've figured out that card fraud beats holding up someone at gunpoint. Instead, they're hacking into Internet databases filled with customer card data and copying account details encoded on a card's magnetic stripe. "Credit card fraud is the bank robbery of the future," says Gregory Regan, special agent in charge of the financial crimes division of the U.S. Secret Service. "[Criminals] have realized that credit cards and the banking system are easy pickings."

Not surprisingly, the Internet is fueling such fraud.

It not only helps criminals retrieve account data quickly and efficiently, but it allows them to perpetrate scams from anywhere in the world. Thieves can E-mail account information overseas to cohorts, who then produce counterfeit cards. Or items can be purchased from an Internet merchant, allowing the fraudster to cloak his identity and leave few clues to track him down. "Any time you are in a non-face-to-face environment, it always makes it easier for fraud," says Rich Detura, director of fraud policy for Citibank.

Easy prey. The astounding growth in electronic-commerce sites provides criminals with a world of merchants to patronize for products that are easily fenced. "No matter how somebody might get ahold of a consumer's financial information, the ability to abuse it on the Internet is huge," says Susan Grant, director of the National Fraud Information Center in Washington.

According to the U.S. Secret Service, the fastest-growing ploy used by criminals–particularly organized groups overseas–is to nab card data by "skimming" them off a genuine card. The magnetic stripe on the card's back is encoded with a cardholder's name, account number, expiration date–and a code unique to each piece of plastic. Without the last number, the card cannot be counterfeited. But thieves are buying magnetic stripe readers–available for about $400 on the Internet–and altering them to record *all* of the data on a magnetic stripe with a mere swipe of the card.

Last November, for example, a Bloomingdale's shopper in New York paying for sunglasses with a credit card noticed something fishy. The card was swiped twice, once through the store's credit card device and also through a store vendor's Palm organizer, which had a skimming device attached

to it. Law enforcement authorities often see this ploy at restaurants, where a dishonest waiter or waitress will unobtrusively pull the small device out of his or her pocket, swipe the card, and hide it before anyone's the wiser.

Some criminals set their sights higher. Recently, a computer hacker obtained thousands of credit card numbers of CD Universe Web site customers and published them on the Internet after the company refused to pay a ransom. "CD Universe basically left the storefront open," says Raf Sorrentino, vice president of fraud and risk management at First Data Corp., an electronic payment processor in Atlanta. The company says security is important, and "obviously it will be even more paramount now," says Brett Brewer, vice president of electronic commerce for eUniverse, which owns CD Universe. Yet experts contend that the firms are partly to blame. "We have companies rushing online trying to cash in on this E-commerce craze and not paying enough attention to security," says Elias Levy, chief technology officer of SecurityFocus.com, a Web information security firm in San Mateo, Calif.

Numbers game. A less sophisticated method of filching card numbers is the many software programs, found free on the Web, that generate numbers using the same algorithms as those used by banks. Anyone with modest computer skills can produce up to 999 card numbers from one card, says Mark Batts, supervisory special agent with the FBI's financial institutions fraud unit. Early last year, the Federal Trade Commission charged several individuals and businesses with illegally billing 783,947 credit and debit card accounts for Internet services. How did the companies get the information? From a bank, which sold them the numbers.

Of course, thieves still acquire credit card

numbers the old-fashioned way, such as dumpster diving and stealing mail. Federal law caps credit card liability at $50 in fraudulent charges. With a credit card, it's not your money at risk. But if someone uses your debit card number, the funds in your checking, savings, or brokerage account–whatever the number is tied to–can be drained. And your line of credit is up for grabs, too. Meanwhile, checks bounce and insufficient-funds fees pile up, and you're left to sort out the damage.

Such a predicament can exact an emotional toll. Leitha Foote's bank didn't quibble when someone withdrew $192 last month from the Dallas woman's checking account using her debit card number. It returned the money immediately, pending an investigation, and canceled the card. "I have no idea how anybody else got the card number," says Foote. "I feel very violated." Consequently, Foote now questions the wisdom of a debit card, which she had liked using to easily pay recurring monthly bills. "This has made me really second-guess whether I am going to continue that convenient lifestyle," says Foote.

Preventing scammers from getting their mitts on your card number is a lot tougher than safeguarding the plastic. "There is not a whole lot the consumer can do," says Wesley Wilhelm, director of consulting for eHNC, a subsidiary of HNC Software, a fraud detection and prevention provider in San Diego. Still, consumers should be cautious about disclosing their card number–never giving it to a caller claiming to be, say, your banker, or to a Web site that appears lax in its security. And try to watch your card whenever it's being swiped.

Fraud alarm. Most important, review your account statements carefully, and notify your bank immediately of any discrepancies. "Look at that

statement the minute it comes," says Linda Sherry, editorial director of Consumer Action in San Francisco. Jim Smith of Milwaukee learned that the hard way. He failed to spot three withdrawals of $19.95 from his checking account via his debit card number in 1998. He finally discovered them when a fourth withdrawal was made last year, causing a check to bounce. While his bank reimbursed him for the latest withdrawal, it refused to compensate him for the earlier ones, saying he had waited too long to notify the bank. "I pay closer attention to my statements now," says Smith. "I go every week and do a balance check on my account at the ATM to make sure everything is OK." (After *U.S. News* called Smith's bank in reporting this story, it agreed to reimburse him for the earlier withdrawals.)

Though the credit card industry empathizes with victims, it says it has been getting a handle on fraud. While skimming has increased in recent years, "the growth has not been what we consider explosive," says John Shaughnessy, senior vice president of risk management for Visa U.S.A. Neural network systems, which can pick up suspicious cardholder usage patterns, and other high-tech measures are helping the issuers combat fraud.

Still, no detection system is foolproof, and the industry has several new fixes on the drawing board. Visa and MasterCard have introduced another validation code, printed on the back of the card, which merchants who accept "card not present" transactions can request of cardholders. Other solutions include technology that will read the properties of the magnetic stripe.

The associations are also working with merchants to help detect fraud in phone and Internet transactions. After all, it's the retailer who gets stuck with the fake transaction. "Typically, the

merchant ends up eating that," says Robert McKinley, president of CardWeb, a Gettysburg, Pa., firm that researches credit cards. Meanwhile, the industry is pushing for widespread adoption of a secure electronic transaction protocol which would create a digital ID for cardholders and merchants. Issuers are weighing in, too. Citibank cardholders, for example, can sign up for "ClickCredit," a separate line of credit and account number to be used exclusively for online buys. Other firms are creating secure payment methods, such as virtual "wallets" for Web purchases.

In the future, many worry that more card fraudsters will go a step further. Identity theft is a huge problem, and a clever con artist can use account information to establish a parallel identity. Victims of fraud are quickly learning the trade-offs of whiz-bang technology. "Privacy is a rare bird these days and becoming much more rare every time we invite someone to access our personal information for the sake of convenience," says Foote. It's a lesson all cardholders should heed.

Back to Top

Exhibit 11

www.csoonline.com/metrics/viewmetric.cfm?id=502

Most Internet Users Want Alternative to Credit Cards

By Jon Surmacz

May 8, 2003

The majority of U.S. Internet users (**61 percent**) say they would be more likely to make online purchases if there was an alternative to using their credit cards. Although **59 percent** of users have purchased some form of Internet content (classified ads, news, music or games), **53 percent** said they'd be more likely to make purchases if there were more secure payment options. It's currently estimated that **83 percent** of Web users have credit cards.

SOURCE: Javelin Strategy & Research, eContent Magazine, PaymentOne, Jupiter Research

At Least Half of Online Consumers Fear Fraud

By Jon Surmacz

December 16, 2003
More than half of online consumers (**52 percent**) say they are at least somewhat more concerned about using their credit card online this holiday season than last year. Identity theft is the No. 1 concern for consumers (**54 percent**) followed by credit card theft (**26 percent**).

SOURCE: SPSS

Fraudulent E-Commerce Transactions Reach 6.2 Percent

By Jon Surmacz
Fraudulent e-commerce transactions comprised **6.2 percent** of e-commerce transactions through August 2003. The United States leads all countries by a large margin in terms of attempted fraud transactions, accounting for **47.8 percent** of worldwide fraud attempts. The United Kingdom was second at **5.25 percent** followed by Nigeria (**4.81 percent**), Canada (**4.66 percent**) and Israel (**4.46 percent**).

SOURCE: Verisign
November 14, 2003

27 Million Americans Affected by Identity Theft

By Jon Surmacz

September 4, 2003

More than 27 million Americans have been victims of identity theft over the last five years, including **9.9 million** in the last year. Losses attributed to identity theft totaled nearly **$48 billion** for businesses in the last year while consumer victims reported **$5 billion** in out-of-pocket expenses. The average business loss to identity theft was **$4,800**. The average consumer loss was **$500**.

Losses From Identity Theft To Total $221 Billion Worldwide

By Jon Surmacz

May 23, 2003

Identity theft will result in the loss of **$221 billion** worldwide by the end of 2003, with **$73.8 billion** lost in the U.S. alone. That number equals the total losses from 2002, when identity theft caused **$73.8 billion** in losses worldwide, with the U.S. accounting for about a third of that with **$24.6 billion**. By 2005, losses from identity theft could amount to **$2 trillion** worldwide, if the **300 percent** compound annual growth rate continues.

SOURCE: Aberdeen Group

Fraud Complaints Triple

By Jon Surmacz
U.S. Internet fraud complaints to federal, state and local agencies tripled from **16,775** to **48,252** between December 31, 2001 and December 31, 2002. **Almost half (46 percent)** of referred complaints dealt with Internet auction fraud, while close to **one-third (31 percent)** were about non-delivery of merchandise and non-payment. The highest median dollar loss was **$3,864**, which came from victims of Nigerian letter fraud. That was followed by those whose identity had been stolen (**$2,000** median loss) and check fraud victims (**$1,100**).

April 9, 2003

Most Online Buyers Worried About Credit Card Data

By Jon Surmacz

February 13, 2003

Among American consumers age 18 and over, **92.4 percent** were either somewhat or very or extremely concerned about the security of their credit card information when purchasing online in 2002. That's a slight decrease from 2001, when **94.4 percent** said they were somewhat or very or extremely concerned. However, concern among consumers about access to their personal information when purchasing online dropped significantly between 2001 and 2002, with **88.8 percent** of persons age 16 or over expressing some concern in 2002, as opposed to **94.6 percent** the year before.

SOURCE: The UCLA Internet Report from the Center for Communication Policy at UCLA

Fraud To Cost Retailers $500 Million During the Holidays

By Jon Surmacz

December 19, 2002

Credit card fraud causes online retailers to lose around **1 percent** of transaction volume and sales revenues. It's predicted that the loss of sales because of fraud and suspect purchases will cost online retailers **$500 million** during the holiday season this year. About **6 percent** of sales are rejected because they're considered suspect, but up to **one-third** of those rejections may be mistakes. In total, fraud will cost retailers **$160 million** from October to December 2002. Suspect sales mistakes will have cost retailers up to **$315 million** in the fourth quarter of 2002.

SOURCE: GartnerGroup

Most Americans have Internet-security concerns

By Jon Surmacz

December 13, 2001

More than **70%** of Americans are concerned about Internet security. Another **74%** are worried about what may happen to their personal information over the Internet. More than half (**71%**) expressed at least "some" faith in the U.S. government to prevent cyber attacks.

SOURCE: Information Technology Association of America

Exhibit 12

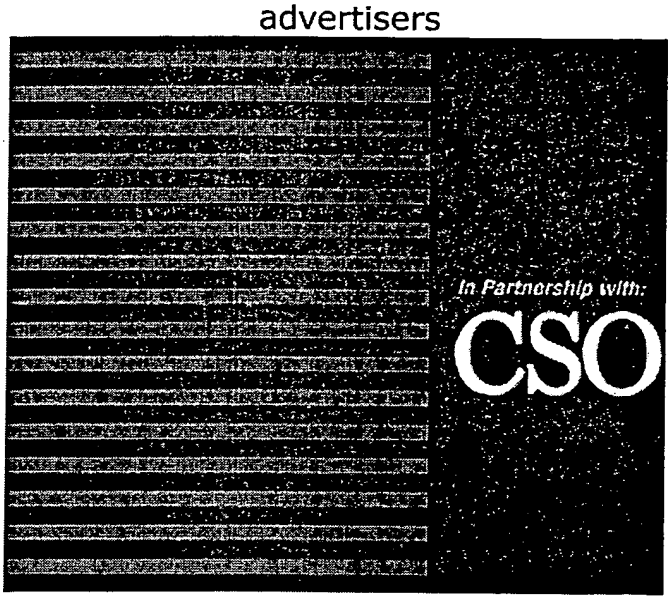
Safety in Numbers

More than 80% of online shoppers fear credit card fraud

By Jon Surmacz

June 21, 2001

Consumers say that they believe their credit card is **12** times more likely to be defrauded online than offline. However, data suggests that the actual occurrence of online fraud is just **three** or **four** times that of offline fraud.



Most consumers listed fraud as three of their top concerns of shopping online as **81%** worry about their credit card numbers being intercepted, **77%** fear that personal data will be sold and **59%** are concerned that their credit card data will be "misused."

SOURCE: Jupiter Media Metrix

Recent Metrics

Most online consumers believe their passwords are secure, but almost half of the never change their passwords. (Dec 18,2003)
Read More

Identity theft and credit card theft top consumer fraud fears this holiday season. (Dec 16,2003)
Read More

The United States leads the world in e-commerce fraud, generating 47.8 percent of worldwide fraudulent transactions. (Nov 14,2003)
Read More

Nearly three in four health care companies don't bother to justify information security spending. (Nov 07,2003)
Read More

Uncle Sam seeks IT workers with security clearance and basic programming skills (Oct 08,2003)
Read More

More digital attacks originate from Brazil than anywhere else; so far the 2003 count stands at more than 95,000 digital attacks. (Sep 26,2003)
Read More

Product related e-mails account for 20 percent of all spam, but Internet related messages show biggest increase. (Sep 17,2003)
Read More

Business Process Management tools gain traction in the enterprise. (Sep 17,2003)
Read More

The FTC projects 210 million complaints reported to its identity theft clearinghou by year-end 2003. (Sep 12,2003)
Read More

Businesses and consumers lose more than $50 billion to identity theft over the la five years. (Sep 04,2003)
Read More

A majority of U.S. companies did not have formal plans in place to handle recent blackouts in the eastern United States. (Aug 28,2003)
Read More

The majority of Fortune 1000 execs are better prepared than they were two year ago to recover from a disaster. (Aug 14,2003)
Read More

Message security market will grow to $1.1 billion by 2007. (Aug 07,2003)
Read More

Security incidents in 2003 on pace to increase 86 percent over 2002. (Jul 31,2003)
Read More

WLANs continue to creep in to the enterprise, but security concerns hamper widespread adoption (Jul 30,2003)
Read More

Many PDA users keep sensitive business information on their PDAs. (Jul 25,2003)
Read More

More than one-third of Canadians say their personal information has been compromised online. (Jul 23,2003)
Read More

Web application security products and services market to hit $1.74 billion by 2007. (Jul 17,2003)

Read More

Global financial firms spend about 6 percent of their IT budgets on security; man have increased staff since 2001. (Jul 10,2003)
Read More

Corporate losses caused by spam will grow from nearly 10-fold from 2003 to 2007. (Jun 20,2003)
Read More

Most broadband users store confidential information on their computers but lack proper firewall protection. (Jun 19,2003)
Read More

Security concerns top list of barriers for online banking. (Jun 13,2003)
Read More

North America was the main source for global security incidents and attacks from the fourth quarter of 2002 through the first quarter of 2003. (Jun 09,2003)
Read More

U.S. consumers to lose $73.8 billion to identity theft. (May 23,2003)
Read More

Chinese developers see spike in security breaches. (May 20,2003)
Read More

More than half of Web shoppers want more secure payment options. (May 08,2003)
Read More

Storing data is the easy part; recovering data is another story. (May 07,2003)
Read More

Klez.E attacks have dropped over last year, but the virus remains one of the mos popular. (May 01,2003)
Read More

Spam attacks increased 4 percent from February to March. (Apr 24,2003)
Read More

Nearly 50,000 Internet fraud incidents were reported in 2002. (Apr 09,2003)
Read More

Nearly one-third identity thefts lead to credit card fraud. (Apr 03,2003)
Read More

Just 42 percent of consumers think businesses handle personal information in a proper and confidential way. (Mar 28,2003)
Read More

Nearly one-third of virus attacks in February can be blamed on the Klez.E worm. (Mar 13,2003)
Read More

One in three companies would lose critical data or operational capability during a disaster because their recovery plans are not adequately funded. (Mar 12,2003)
Read More

Digital attacks against U.S., U.K. on the rise. (Mar 06,2003)
Read More

Less than half of companies have intrusion detection systems in place. (Feb 27,200
Read More

Many IT professionals expect military forces or terrorists to launch a large-scale cyberattack within two years. (Feb 20,2003)
Read More

The United States was the number-one target of hackers in 2002. (Feb 14,2003)
Read More

Protecting credit card information during online purchases is of concern to 92.4 percent of Web shoppers. (Feb 13,2003)
Read More

Damages from digital attacks total $8 billion in January. (Feb 06,2003)
Read More

Companies rank virus threats as top security priority for 2003. (Jan 29,2003)
Read More

Online auctions account for half of Internet fraud complaints. (Jan 24,2003)
Read More

Fridays and weekends are prime-time for hackers. (Jan 23,2003)
Read More

Retailers lose about 1 percent of transaction volume to credit card fraud. (Dec 19,2002)
Read More

More than 7,000 viruses detected this year (Dec 12,2002)
Read More

Three percent of online sales will be lost because of credit card fraud. (Dec 05,2002
Read More

A recent survey finds that investments in identity management technologies can pay off, but few companies are investing. (Nov 26,2002)
Read More

Security and business continuity a top priority for 29 percent of companies in 2003. (Nov 21,2002)
Read More

Most Web shoppers are concerned about their personal information being sold or stolen. (Nov 15,2002)
Read More

Of U.K. companies that allow remote access to company networks, 52 percent ar worried about security problems. (Nov 15,2002)
Read More

More than 40 percent of companies spend 5 percent or more of their IT budget o security. (Oct 30,2002)
Read More

Internet attacks against public and private organizations jumped 28 percent from January to June 2002. (Oct 24,2002)
Read More

One in every 24 e-mail received by U.K. retailers contains a virus. (Oct 17,2002)
Read More

The vulnerability scanning and assessment market will thrive as CIOs seek security help outside the organization. (Oct 09,2002)
Read More

More government websites are posting privacy and security policies. (Oct 04,2002)
Read More

Just 30 percent of Canadian CEOs think their security measures are effective. (Oc 03,2002)
Read More

Just one in five U.S. companies rates crisis preparedness a priority (Sep 25,2002)
Read More

More than 80 percent of U.S. security professionals fear hacker attacks on their networks. (Sep 19,2002)
Read More

Unless security issues are resolved, Bluetooth may remain a niche technology in the enterprise (Sep 11,2002)
Read More

Nearly one-third of companies say they don't have adequate plans for combattin cyberterrorism. (Sep 10,2002)
Read More

IT professionals fear a cyberattack by terrorists within two years. (Aug 23,2002)
Read More

Roughly 180,000 Internet-based attacks hit U.S. businesses in first half of 2002. (Jul 09,2002)
Read More

Nearly all consumers say disclosure is important for e-commerce websites. (Jun 25,2002)
Read More

Most online consumers are willing to trade personal info for rewards. (Jun 04,2002)
Read More

Why ROI is the wrong question to ask about security (May 08,2002)
Read More

More than 49,000 complaints of Internet fraud filed in 2001. (Apr 10,2002)
Read More

Nearly 75 percent of U.S. websites have a privacy policy. (Apr 04,2002)
Read More

New markets push spending on corporate protection. (Mar 27,2002)
Read More

Chief security officers who report to the CFO make twice as much as those who report to the CIO. (Mar 26,2002)
Read More

By 2005, worldwide market for firewalls will hit $3.8 billion, up from $1.7 billion i 2001. (Mar 08,2002)
Read More

Most Americans are concerned about Internet security; 74% are worried about their personal info. (Dec 13,2001)
Read More

Most (64%) people don't pay attention to privacy policies. (Dec 04,2001)
Read More

More than two-thirds of e-retailers are taking extra precautions against fraud this year. (Nov 20,2001)
Read More

Reports on inside security breaches up 7 percentage points over 2000. (Oct 16,200
Read More

Many companies aren't prepared for dealing with disruption. (Sep 26,2001)
Read More

Most marketing companies have a CPO; nearly half use consultants. (Sep 13,2001)
Read More

Employers look to employee Internet monitoring to stem liability and security issues. (Sep 12,2001)
Read More

Companies spend $140 million per year worldwide to monitor employee Internet, e-mail use. (Jul 10,2001)
Read More

Just 16 percent of managers and IT staffers surveyed said that their companies were members of an industry consortium that addressed privacy issues. (Jun 20,2001)
Read More

Security incidents surpass 7,000 in Q1 2001; on pace to eclipse 2000 figure. (Ma

01,2001)
Read More

The secure content delivery market will reach $2 billion by 2005. (Apr 03,2001)
Read More

Two reports show businesses and consumers still wary of blowing the whistle (Ma 14,2001)
Read More

Security breaches occur at 85% of U.S. businesses and government organization (Mar 13,2001)
Read More

Increased awareness means that European and U.S. firms will boost security spending. How much depends on what companies are willing to risk. (Feb 08,2001)
Read More

Increased awareness means that European and U.S. firms will boost security spending. How much depends on what companies are willing to risk. (Feb 07,2001)
Read More

Spending on security will grow from $8.7 billion to $30.3 billion worldwide. (Jan 25,2001)
Read More

Consumers want companies to ask permission before taking personal data. (Oct 12,2000)
Read More

Return to Metrics Index

Exhibit 13

Safety in Numbers

Most Internet Users Want Alternative to Credit Cards

By Jon Surmacz

May 8, 2003

The majority of U.S. Internet users (**61 percent**) say they would be more likely to make online purchases if there was an alternative to using their credit cards. Although **59 percent** of users have purchased some form of Internet content (classified ads, news, music or games), **53 percent** said they'd be more likely to make purchases if there were more secure payment options. It's currently estimated that **83 percent** of Web users have credit cards.

SOURCE: Javelin Strategy & Research, eContent Magazine, PaymentOne, Jupiter Research

Recent Metrics

Most online consumers believe their passwords are secure, but almost half of the never change their passwords. (Dec 18,2003)
Read More

Identity theft and credit card theft top consumer fraud fears this holiday season. (Dec 16,2003)
Read More

The United States leads the world in e-commerce fraud, generating 47.8 percent of worldwide fraudulent transactions. (Nov 14,2003)
Read More

Nearly three in four health care companies don't bother to justify information

security spending. (Nov 07,2003)
Read More

Uncle Sam seeks IT workers with security clearance and basic programming skills (Oct 08,2003)
Read More

More digital attacks originate from Brazil than anywhere else; so far the 2003 count stands at more than 95,000 digital attacks. (Sep 26,2003)
Read More

Product related e-mails account for 20 percent of all spam, but Internet related messages show biggest increase. (Sep 17,2003)
Read More

Business Process Management tools gain traction in the enterprise. (Sep 17,2003)
Read More

The FTC projects 210 million complaints reported to its identity theft clearinghous by year-end 2003. (Sep 12,2003)
Read More

Businesses and consumers lose more than $50 billion to identity theft over the la five years. (Sep 04,2003)
Read More

A majority of U.S. companies did not have formal plans in place to handle recent blackouts in the eastern United States. (Aug 28,2003)
Read More

The majority of Fortune 1000 execs are better prepared than they were two year ago to recover from a disaster. (Aug 14,2003)
Read More

Message security market will grow to $1.1 billion by 2007. (Aug 07,2003)
Read More

Security incidents in 2003 on pace to increase 86 percent over 2002. (Jul 31,2003)
Read More

WLANs continue to creep in to the enterprise, but security concerns hamper widespread adoption (Jul 30,2003)
Read More

Many PDA users keep sensitive business information on their PDAs. (Jul 25,2003)
Read More

More than one-third of Canadians say their personal information has been compromised online. (Jul 23,2003)
Read More

Web application security products and services market to hit $1.74 billion by 2007. (Jul 17,2003)
Read More

Global financial firms spend about 6 percent of their IT budgets on security; man have increased staff since 2001. (Jul 10,2003)
Read More

Corporate losses caused by spam will grow from nearly 10-fold from 2003 to 2007. (Jun 20,2003)
Read More

Most broadband users store confidential information on their computers but lack proper firewall protection. (Jun 19,2003)
Read More

Security concerns top list of barriers for online banking. (Jun 13,2003)
Read More

North America was the main source for global security incidents and attacks from the fourth quarter of 2002 through the first quarter of 2003. (Jun 09,2003)
Read More

U.S. consumers to lose $73.8 billion to identity theft. (May 23,2003)
Read More

Chinese developers see spike in security breaches. (May 20,2003)
Read More

Storing data is the easy part; recovering data is another story. (May 07,2003)
Read More

Klez.E attacks have dropped over last year, but the virus remains one of the mos popular. (May 01,2003)
Read More

Spam attacks increased 4 percent from February to March. (Apr 24,2003)
Read More

Nearly 50,000 Internet fraud incidents were reported in 2002. (Apr 09,2003)
Read More

Nearly one-third identity thefts lead to credit card fraud. (Apr 03,2003)
Read More

Just 42 percent of consumers think businesses handle personal information in a proper and confidential way. (Mar 28,2003)
Read More

Nearly one-third of virus attacks in February can be blamed on the Klez.E worm. (Mar 13,2003)
Read More

One in three companies would lose critical data or operational capability during a disaster because their recovery plans are not adequately funded. (Mar 12,2003)
Read More

Digital attacks against U.S., U.K. on the rise. (Mar 06,2003)

Read More

Less than half of companies have intrusion detection systems in place. (Feb 27,2003
Read More

Many IT professionals expect military forces or terrorists to launch a large-scale cyberattack within two years. (Feb 20,2003)
Read More

The United States was the number-one target of hackers in 2002. (Feb 14,2003)
Read More

Protecting credit card information during online purchases is of concern to 92.4 percent of Web shoppers. (Feb 13,2003)
Read More

Damages from digital attacks total $8 billion in January. (Feb 06,2003)
Read More

Companies rank virus threats as top security priority for 2003. (Jan 29,2003)
Read More

Online auctions account for half of Internet fraud complaints. (Jan 24,2003)
Read More

Fridays and weekends are prime-time for hackers. (Jan 23,2003)
Read More

Retailers lose about 1 percent of transaction volume to credit card fraud. (Dec 19,2002)
Read More

More than 7,000 viruses detected this year (Dec 12,2002)
Read More

Three percent of online sales will be lost because of credit card fraud. (Dec 05,2002
Read More

A recent survey finds that investments in identity management technologies can pay off, but few companies are investing. (Nov 26,2002)
Read More

Security and business continuity a top priority for 29 percent of companies in 2003. (Nov 21,2002)
Read More

Most Web shoppers are concerned about their personal information being sold or stolen. (Nov 15,2002)
Read More

Of U.K. companies that allow remote access to company networks, 52 percent ar worried about security problems. (Nov 15,2002)
Read More

More than 40 percent of companies spend 5 percent or more of their IT budget on security. (Oct 30,2002)
Read More

Internet attacks against public and private organizations jumped 28 percent from January to June 2002. (Oct 24,2002)
Read More

One in every 24 e-mail received by U.K. retailers contains a virus. (Oct 17,2002)
Read More

The vulnerability scanning and assessment market will thrive as CIOs seek security help outside the organization. (Oct 09,2002)
Read More

More government websites are posting privacy and security policies. (Oct 04,2002)
Read More

Just 30 percent of Canadian CEOs think their security measures are effective. (Oc 03,2002)
Read More

Just one in five U.S. companies rates crisis preparedness a priority (Sep 25,2002)
Read More

More than 80 percent of U.S. security professionals fear hacker attacks on their networks. (Sep 19,2002)
Read More

Unless security issues are resolved, Bluetooth may remain a niche technology in the enterprise (Sep 11,2002)
Read More

Nearly one-third of companies say they don't have adequate plans for combatting cyberterrorism. (Sep 10,2002)
Read More

IT professionals fear a cyberattack by terrorists within two years. (Aug 23,2002)
Read More

Roughly 180,000 Internet-based attacks hit U.S. businesses in first half of 2002. (Jul 09,2002)
Read More

Nearly all consumers say disclosure is important for e-commerce websites. (Jun 25,2002)
Read More

Most online consumers are willing to trade personal info for rewards. (Jun 04,2002)
Read More

Why ROI is the wrong question to ask about security (May 08,2002)
Read More

More than 49,000 complaints of Internet fraud filed in 2001. (Apr 10,2002)
Read More

Nearly 75 percent of U.S. websites have a privacy policy. (Apr 04,2002)
Read More

New markets push spending on corporate protection. (Mar 27,2002)
Read More

Chief security officers who report to the CFO make twice as much as those who report to the CIO. (Mar 26,2002)
Read More

By 2005, worldwide market for firewalls will hit $3.8 billion, up from $1.7 billion i 2001. (Mar 08,2002)
Read More

Most Americans are concerned about Internet security; 74% are worried about their personal info. (Dec 13,2001)
Read More

Most (64%) people don't pay attention to privacy policies. (Dec 04,2001)
Read More

More than two-thirds of e-retailers are taking extra precautions against fraud this year. (Nov 20,2001)
Read More

Reports on inside security breaches up 7 percentage points over 2000. (Oct 16,2001
Read More

Many companies aren't prepared for dealing with disruption. (Sep 26,2001)
Read More

Most marketing companies have a CPO; nearly half use consultants. (Sep 13,2001)
Read More

Employers look to employee Internet monitoring to stem liability and security issues. (Sep 12,2001)
Read More

Companies spend $140 million per year worldwide to monitor employee Internet, e-mail use. (Jul 10,2001)
Read More

Consumers say they are 12 times more likely to be defrauded online than offline. (Jun 21,2001)
Read More

Just 16 percent of managers and IT staffers surveyed said that their companies were members of an industry consortium that addressed privacy issues. (Jun 20,2001)
Read More

Security incidents surpass 7,000 in Q1 2001; on pace to eclipse 2000 figure. (May 01,2001)
Read More

The secure content delivery market will reach $2 billion by 2005. (Apr 03,2001)
Read More

Two reports show businesses and consumers still wary of blowing the whistle (Mar 14,2001)
Read More

Security breaches occur at 85% of U.S. businesses and government organizations (Mar 13,2001)
Read More

Increased awareness means that European and U.S. firms will boost security spending. How much depends on what companies are willing to risk. (Feb 08,2001)
Read More

Increased awareness means that European and U.S. firms will boost security spending. How much depends on what companies are willing to risk. (Feb 07,2001)
Read More

Spending on security will grow from $8.7 billion to $30.3 billion worldwide. (Jan 25,2001)
Read More

Consumers want companies to ask permission before taking personal data. (Oct 12,2000)
Read More

Return to Metrics Index

Exhibit 14

Security

When it comes to customer security, no one is more serious than NextCard Visa. We have designed one of the safest and most error-free systems around. To double check our security, we engaged PriceWaterhouseCoopers as independent security auditors to give us a clean bill of health. Our policy is to conduct regular third-party audits of our security to ensure that our standards never slip.

We'll walk you through our security, section by section, to let you know how we're protecting you. The NextCard Visa ensures that you are:

- Protected against somebody stealing your personal data
- Protected against electronic eavesdropping
- Protected against intercepted email
- Protected against hackers using your stolen credit card numbers
- Protected against failed security

Go Back

Protected against somebody stealing your personal data TOP

Your private account information is stored on an isolated NextCard Visa computer called a Customer Information Server. This server is carefully protected both physically and electronically.

Physically, the server is stored in a highly secure building maintained by Exodus Communications Inc., whose mission is to provide the highest degree of security for Internet applications. Key features of Exodus security:

- ***Fire Suppression System*** - State-of-the-art gas-based fire protection system, separate fire zones below the floor and above the ceiling, specialized heat/smoke sensors, and automatic local fire department notification
- ***Facility Security System*** - Motion sensors, secured access, video camera surveillance, security breach alarm, and 24 X 7 automatic local police department notification

- ***Personal Security System*** - 24 X 7 card key customer access to Internet Data Centers, monitoring, and 24 X 7 on-site personnel
- ***Server Cage*** - Our server is locked in a steel wire cage inside the secured Exodus building

Electronically, your private account information is NOT directly connected to the Internet. It sits behind a firewall. The firewall ensures that the sensitive information stored on the customer server is not available to unauthorized computers. It only allows certain messages from authorized computers through. The firewall we are using is a recognized industry standard, and exceeds the standards set by the International Computer Security Association (ICSA), a leading industry authority on the issue of Internet security.

Protected against electronic eavesdropping TOP

You communicate with NextCard Visa through your computer's web browser. Your browser is a critical piece of our security infrastructure. We only support browsers that use Secure Sockets Layer (SSL) 3.0 or higher.

Your browser will handle these interactions automatically, so you do not have to take any extra steps to be protected. In fact, before you login or fill out an application, our server checks to make sure you're using one of the approved browsers.

SSL 3.0 provides protection against electronic eavesdropping through:

1. ***Server Authentication*** -- Secure Sockets Layer 3.0 provides a way for you to verify that you are in fact logging on to the NextCard Visa server and not a site that is impersonating our server. Before you logon to NextCard Visa, our server sends NextCard Visa's public key to your browser program. SSL 3.0, lets you verify the identity of a server by viewing the site's Certificate. A Certificate is a way of associating a public key to a name. You can be sure that you are logged on to the NextCard Visa server by viewing our Certificate through your browser program when you're on the first page of the online application or login screen.
2. ***Data Encryption*** - Once SSL has authenticated the server, your browser and our server will establish a secret symmetric key. The symmetric key allows your browser and our server to exchange encrypted data. The symmetric key is valid for a single session only. If you log out and later come back to NextCard Visa, your browser and our server will negotiate a different symmetric key automatically. The symmetric key protects all of your communications with NextCard Visa.
3. ***Message Authentication Code*** - With data encryption in place, no outside party can understand our communications, but they

could still intercept a message and scramble it. To detect message tampering, SSL uses a message authentication code (MAC). A MAC is a piece of data that is computed, using pieces of the symmetric key and the message itself. Your browser always checks the MAC before interpreting a message from our server. If the message was scrambled by a hacker, the MAC would not correctly compute and your browser will alert you of possible security hazards. The chances of someone scrambling a message and then guessing the correct MAC are pretty slim: about 1 in 18,446,744,073,709,551,616 under 128-bit encryption.

Protected against intercepted email TOP

E-mail is a great way to pass messages, but it is not a secure communication channel. Here at NextCard Visa, all customer messages travel through SecureMail(sm), our secured, web-based communication system. Each of our customers has a personal SecureMail(sm) box that is easily accessible within our customer service website. And because SecureMail(sm) is entirely web-based, there's no need to learn a new email program or download additional software. SecureMail(sm) uses SSL 3.0 to protect all confidential communication.

Protected against hackers using your stolen credit card numbers TOP

In the wrong hands, technology has a way of distorting reality. For example, suppose you buy something with your NextCard Visa from an Internet merchant who turns out not to be a merchant, but a clever thief. The merchant website looked like a legitimate business and you took all the right precautions. But still, the hacker got your credit card number.

It is impossible to guarantee that an Internet thief will never get your NextCard Visa number, but we DO guarantee that you will not have to pay for any charges he rings up.

Here's our ***100% Safe Internet Shopping Pledge***[sm]: We will cover the full cost of any fraud against your account that arises from your usage of a NextCard Visa over the Internet. Shop online risk FREE and rest assured that you will not be held responsible for fraudulent charges to your NextCard Visa incurred by someone else.

Protected against failed security TOP

Technology moves forward at a rapid pace. The thieves get smarter, and so do the security systems. No matter what happens, you are always protected against security breaches with our ***100% Safe Internet Shopping Pledge***[sm].


Go Back

Introduction
How it Works
Shop
Card Issuers
FAQs

Privacy & Security
Terms & Conditions

How It Works

Overview | Demo of Shopping with Verified by Visa

Verified by Visa protects your existing Visa card with a password you create, giving you reassurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

How it Works: Activating your card

How it Works: Shopping with Verified by Visa

How it Works: Activating your card

You may activate Verified by Visa for your Visa card in two ways: *Activate Now* or *Activate During Shopping*. Details are provided below.

Activate now.
You may activate now by entering your card number over our secure server. If your card issuer is participating in Verified by Visa (most issuers are) you'll complete a brief activation process. You'll verify your identity, create your Verified by Visa password and you're done.

Activate during shopping.

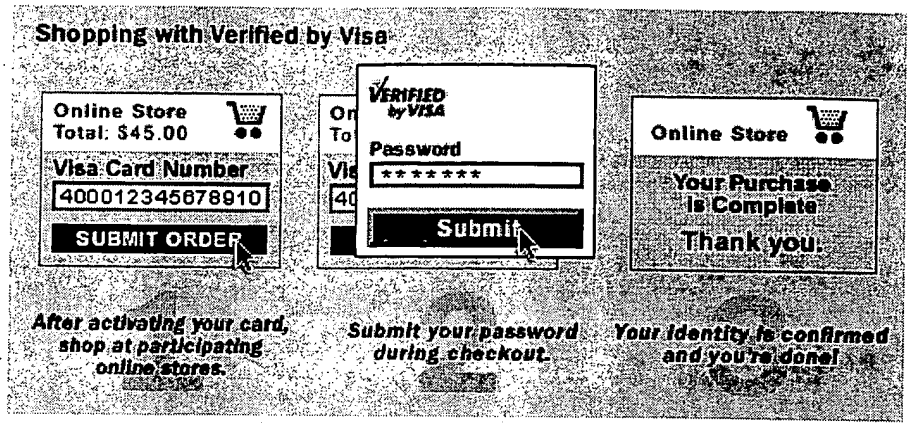
Activating your card during shopping is quick and easy.
Your Visa card issuer may also set-up your card to be eligible to activate while shopping. During checkout at participating online stores you may encounter a message offering the opportunity to activate Verified by Visa for your Visa card.

If you choose to activate during shopping, you'll provide information to your Visa card issuer to confirm your identity and then create your password. On future purchases at participating online stores your Verified by Visa password will be required during checkout, ensuring your added safety.

Back to Top

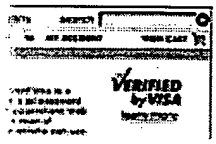
How it Works: Shopping with Verified by Visa

See a demo of how Verified by Visa protects you while shopping online.



Your card is automatically recognized.
Once your card is activated, your card number will be recognized whenever you purchase at participating online stores. You'll enter your password in the Verified by Visa window, your identity will be verified, and the transaction will be completed. In stores that are not yet participating in Verified by Visa, your Visa card will continue to work as usual.

Look for the Verified by Visa symbol displayed at many participating online stores.



Verified by Visa also works with smart Visa cards.

Check Availability

See if Verified by Visa is available for your card. Click Activate Now and submit your card number over our secure server.

Shop with Verified by Visa

See all the great stores where you can shop online with added safety after you activate your card.

Back to Top